Selected Essays on State Open Government Law and Practice in a Post-9/11 World

Jeffrey F. Addicott

Ema Garcia

Jeffrey F. Addicott & Ema Garcia, *Selected Essays on State Open Government Law and Practice in a Post-9/11 World* (2008).

Selected Essays On

State Open Government Law and Practice in a Post-9/11 World

Jeffrey F. Addicott
Ema Garcia

Lawyers & Judges Publishing Company, Inc.
Tucson, Arizona

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

—From a Declaration of Principles jointly adopted by
a Committee of the American Bar Association
and a Committee of Publishers and Associations.

The publisher, editors and authors must disclaim any liability, in whole or in part, arising from the information in this volume. The reader is urged to verify the reference material prior to any detrimental reliance thereupon. Since this material deals with legal, medical and engineering information, the reader is urged to consult with an appropriate licensed professional prior to taking any action that might involve any interpretation or application of information within the realm of a licensed professional practice.

Lawyers & Judges Publishing Company, Inc.
P.O. Box 30040 • Tucson, AZ 85751-0040
(800) 209-7109 • FAX (800) 330-8795
e-mail: sales@lawyersandjudges.com
www.lawyersandjudges.com

ISBN 13: 978-1-933264-50-9
ISBN 10: 1-933264-50-0
Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

ST. MARY'S UNIVERSITY
Center *for* Terrorism Law
SCHOOL OF LAW

Contents

Acknowledgements

The editors wish to acknowledge the invaluable support of Ahsan Nasar who expertly dealt with the conceptual, bibliographical and organizational issues.

Introduction

This compilation of essays was created for a project conducted by the Center for Terrorism Law, St. Mary's University School of Law supported by a 2006 "Congressionally-Directed Homeland Defense and Civil Support Threat Information Collection" grant administered by the Air Force Research Laboratory under agreement FA8750-06-1-0243. This compilation is the result of a discussion had by subject matter experts at the *State Open Government Law and Practice in a Post-9/11 World: Legal and Policy Analysis* symposium held at the National Press Club, Washington, D.C., on November 15 and 16, 2007. This compilation is intended to serve as a companion publication to STATE OPEN GOVERNMENT LAW AND PRACTICE IN A POST-9/11 WORLD: CHANGES IN STATE PUBLIC INFORMATION LAWS IN THE UNITED STATES SINCE THE WAR ON TERRORISM & SELECTED CHANGES IN THE NATIONAL PUBLIC INFORMATION LAWS SINCE THE WAR ON TERRORISM IN COLOMBIA, FRANCE, ISRAEL, AND THE UNITED KINGDOM (Jeffrey F. Addicott, Loren A. Cochran, Lucy A. Dalglish, & Nathan Weingar eds., Lawyers & Judges, 2007) [hereinafter Open Government Guide].

This compilation is organized into chapters that compliment the Open Government Guide. Each chapter consists of papers written by subject matter experts in the appropriate field who elected to participate in the Center for Terrorism Law project. Each author presented their paper and discussed the pertinent topics at the symposium in 2007. The Center for Terrorism Law is a nonprofit, nonpartisan, academic research center. The work presented herein is entirely that of the authors and the ideas, conclusions, and opinions do not reflect those of the Center for Terrorism Law or the Air Force Research Laboratory.

This compilation is separated into seven (7) chapters based on the subject matter. To help the reader understand the focus of each chapter, a short description of the subject of each chapter follows.

Chapter 1 serves as an introduction to the topic of open government laws. The first author discusses the laws that currently exist both at the federal level and in the individual states. The second essay provides a detailed overview of the changes in open government laws in Florida. These essays serve as general summaries of the topics covered by the remainder of the authors.

Chapter 2 is focused on Critical Infrastructure. Critical infrastructure, for the purposes of categorizing essays includes building and architectural plans, vulnerability assessments, energy and public utilities information, mass transit, and telecommunications systems. Most of the authors have defined critical infrastructure as they have used the term in their works.

Chapter 3 is focused on Public Health. Public health in this context includes bioterrorism, medical, pharmaceutical and health laboratory information, hazardous materials, and government response to public health emergencies.

Chapter 4 is focused on Cyber Security. By cyber security, the editors have included geographic information security (GIS) maps, personally identifiable information and identity theft, security investigations, and security procedures, codes, surveillance and cyberterrorism.

Chapter 5 is focused on Political Structure. This broad topic area covers the expanded executive powers; legislation proposed by not yet enacted, confidentiality based on federal regulations, federal programs, or Homeland Security

Commissions; and the closure of otherwise public meetings for security reasons. Many authors discuss the interaction between federal and state laws covering open government in this area and provide insights as to the workings of these laws.

Chapter 6 is focused on Terror Investigations. In this chapter, the author discusses law enforcement investigations, expanded wiretapping powers, and general criminal intelligence information. The author looks to the history of terror investigations and the use of open government information to aid or hinder these efforts.

Chapter 7 is focused on an International Approach to open government laws. The authors take an in depth look at the laws and workings of the Israeli and French open government laws to offer readers an alternate perspective of the issues covered in this book.

Jeffrey F. Addicott and Ema Garcia
San Antonio, Texas, March 2008

Chapter 1

General Overview

Synopsis

1.1 State Law and National Security

by Pete Weitzel

In the wake of 9/11, most of the 50 states wrote new laws designed to deal with the concerns and fears raised by the terrorist attacks on New York's Twin Towers and the Pentagon. The majority of those new laws sought to assure greater security by imposing some measure of greater secrecy, sealing both existing records and new information being gathered about infrastructure, security measures, and response planning. Some states created new governmental units to deal with security issues; others expanded the authority of existing units or made other operational changes.

However, three states – Hawaii, Mississippi and South Dakota – adopted no new laws. The only new law passed in Wisconsin and in Rhode Island dealt with federal information sharing; the only new law in Minnesota allowed for closure of meetings where security matters were discussed. New York's legislature debated exemptions for infrastructure information but in the end simply asked power companies to submit security plans for review. It did approve an exemption for information about information technology assets.

Nevada's new laws may have been the most detailed and comprehensive. The infrastructure protections, for instance, cover not just the usual suspects but the state's gaming establishments – and places of worship.

In many of the states, the laws adopted include individual provisions that fall into several of the six categories selected for separate review in this study. For this overview, we have shortened the provisions into summary descriptions and sorted these by category and subcategory. We hope this will provide a sense of the overall sweep of the laws enacted after 9/11 while allowing for the more detailed analysis of the individual categories sought by the conference sponsors.

State Laws and Infrastructure Security

All but ten states enacted legislation providing, in some manner, for the safeguarding of sensitive information related to their state's infrastructure.

These new laws exempted information falling into one or more broad, sometimes overlapping, categories of information about public and private facilities:

- Building plans and blueprints for public and certain private facilities.
- General security plans developed by agencies and security plans specific to public buildings and public facilities.
- Vulnerability assessments for public and private facilities and for infrastructure, and for companies making or using chemical and other hazardous materials.
- Critical infrastructure risk assessments and protection plans.

Missouri and Ohio, among others, followed the federal pattern and provided exemptions for security plans and vulnerability assessments that are voluntarily submitted by private owners to government agencies for review.

Some states pointed specifically to public water systems, utilities, transportation facilities, or to arenas and stadiums. Delaware passed a law exempting from its public records laws information on telecommunications facilities and switching equipment.

Most of the exemptions laws are broadly written, but several states were quite specific. New Mexico created a single new exemption, for tactical response plans and procedures. Nevada established an exemption for information about "special equipment used in emergency operations." It also limited its vulnerability assessment exemption to analyses involving fire and law enforcement headquarters and critical energy and water infrastructure. Florida protected manuals developed for security personnel. Nebraska's law included only "specific, unique vulnerability assessments." Similarly, West Virginia's new law provided that the vulnerability assessments and security plans being exempted must be specific and unique.

Louisiana was the only state to specifically exempt pipeline security information. With its critical economic dependence on its ports, it also exempted from the public records law information on port security plans, vessel or fleet security plans, port or facility vulnerability assessments, security and safety plans, and "other information related to security plans, procedures, or programs for facilities or vessels." But two other key cargo port states, New York and California, saw no such need.

Indiana lawmakers, perhaps as confused as we by the proliferation of designations for sensitive information, covered all the possible bases, exempting vulnerability assessments, risk planning documents, needs assessments, threat assessments, intelligence assessments, and domestic preparedness strategies.

The language safeguarding security plans was often general but sometimes specifically included both protection and response plans. Iowa's law specified both government security procedures and employee preparedness, and tossed in "codes and combinations, passwords, restricted area passes, keys, security or response procedures; and emergency response protocols."

Kansas wrote into its statute a very broad definition of terrorism security: "criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government." The security measures protected included "intelligence information, tactical plans, resource deployment and vulnerability assessments."

What is the Critical Infrastructure that Needs Protecting?

Most of us, I suppose, would know critical infrastructure when we saw it. But there is no official, or consistent, definition in federal or state law. The critical infrastructure lists that have been drawn might provide some guidance, by showing what has been selected, but these are confidential and not available to anyone without an official need to know.

At one point, the Department of Homeland Security (DHS) produced a list said to be 77,000 infrastructures strong, but when some of the entries leaked, the response was derisive. Rep. Jane Harman, chair of the House Intelligence, Information Sharing and Terrorism Risk Assessment subcommittee, said she didn't think miniature golf courses and public swimming pools warranted a lot of national concern. She called the National Assets Database "almost useless to the private sector and first responders."

At mid-summer, she said she'd been shown a new and improved list at a classified briefing and thought it wouldn't "make people's eyes roll."

The Congressional Research Service offers this lawyerly definition, nicely open to a lot of interpretation: "Systems and assets, the destruction or incapacity of which would:

- cause catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction;
- impair Federal departments and agencies' abilities to perform essential missions or ensure the public's health and safety;
- undermine State and local government capacities to maintain order and deliver minimum essential public services;
- damage the private sector's capability to ensure the orderly functioning of the economy;
- have a negative effect on the economy through the cascading disruption of other critical infrastructure; or
- undermine the public's morale and confidence in our national economic and political institutions.

DHS has compartmentalized critical infrastructure into 17 sectors for both operational and information sharing purposes. If anything, these sector designations just make it that much more difficult to get a handle on what needs to be protected, because the 17 categories sum to nearly everything. The sectors are: Food, Meat and Poultry, Banking and Finance, Drinking Water and Water Treatment Systems, Public Health and Healthcare, National Monuments and Icons, Energy, Industrial Base, Transportation Systems, Postal and Shipping, Information Technology, Communications, Commercial Nuclear Reactors, Materials, and Waste, Chemical, Dams, Commercial Facilities, Government Facilities, Emergency Services, and All Other.

Here's a recap of the exemptions in current state laws covering critical infrastructure:

No Specific Safeguarding Provisions (10)

- Colorado
- Hawaii
- Minnesota
- Mississippi
- New Hampshire
- New York
- Pennsylvania
- Rhode Island
- South Dakota
- Wisconsin

Exemptions for Security Plans (28)

- General to security plans and discussion of security plans. (AL)
- Security plans: Maintaining, or restoring security in the state. (AK)
- Security plans; broadly stated. (CA)
- Internal security audits of government-owned or leased facilities…Security and training manuals. (CT)
- Manuals for security personnel, emergency equipment, or security training…Security system plans for: property owned by or leased to the state or its political subdivisions; or privately owned or leased property held by an agency. (FL)
- Any plan for protection against terrorist or other attacks whose effectiveness depends upon a lack of general public knowledge of details;…security measures, and response policies or plans. (GA)
- Security measures, and response policies or plans. (ID)
- Information on security procedures of government property or emergency preparedness of government employees. Includes vulnerability assessments; security and response plans, codes and combinations, passwords, restricted area passes, keys, and security or response procedures; emergency response protocols. (IA)

- Emergency or security information or procedures of a public agency; Security information on systems, facilities or equipment used in the production, transmission or distribution of energy, water or communications services; Private property or persons, if the records are submitted to the agency. Security means measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government. Security measures include intelligence information, tactical plans, resource deployment and vulnerability assessments. (KA)
- Antiterrorism protective measures and plans; Counterterrorism measures and plans; Security and response needs assessments. (KY)
- Security procedures, terrorist activity intelligence, threat or vulnerability assessments, including physical security information, proprietary information, operational plans, internal security information. (LA)
- Security plans, security procedures or risk assessments prepared specifically for the purpose of preventing or preparing for acts of terrorism. (ME)
- Security and emergency preparedness measures. (MA)
- Security planning, records related to procurement, spending of public funds on security systems. (MO)
- Information on the public safety or security of public facilities, including building plans, alarms systems, and facility staffing. (MT)
- Records related to protection of public property and persons on the property. Specific, unique response plans. (NE)
- Tactical response plans or procedures. (NM)
- Specific emergency response plans, special equipment used in emergency operations, the security of radio-transmission frequencies, information systems vulnerability assessments, security measures, recovery plans. (NV)
- Emergency or security information or procedures for any buildings or facility security measures and surveillance techniques. (NJ)
- Sensitive public security information: Security plans and arrangements; detailed plans and drawings of public buildings and infrastructure facilities; response plans, to the extent such records set forth vulnerability and risk assessments, potential targets, specific tactics, or specific security or emergency procedures. (NC)
- Port and waterway security plans. (OH)
- Records on details for deterrence or prevention of or protection from terrorism. (OK)
- Security Programs of the Energy Facility Citing Council; county elections security plans; utilities, telecommunications, data systems, and hazardous materials. (OR)
- Records classified by an agency that involve security measures to protect persons and property, public or private, including building and public works designs of public facilities. (UT)
- Terrorism prevention and response plans. (VA)
- Protection plans, deployment plans, response plans. (WA)
- Records assembled, prepared or maintained to prevent, mitigate or respond to terrorist acts or the threat of terrorist acts.…Security or disaster recovery plans, risk assessments, tests, or the results of those tests. (WV)
- Safety, security related records of any publicly owned or leased buildings. (WY)

Exemptions for Vulnerability Assessments (20)

- Vulnerability assessments. (CA, ID, IL, WY)

- Any specific vulnerability assessment. (DC)
- Threat assessments, threat response plans. (FL)
- Vulnerability assessments for utilities, technology infrastructure, public buildings, facilities, or activities. (GA)
- Vulnerability assessments; risk planning documents; needs assessments; threat assessments; intelligence assessments; domestic preparedness strategies. (IN)
- Criticality lists (from consequence assessments). Vulnerability assessments. (KY)
- Emergency plans including vulnerability assessments, specific tactics, specific emergency procedures, or specific security procedures. (MD)
- Threat and vulnerability assessments. (MA)
- Specific, unique vulnerability assessments. (NE)
- Vulnerability assessments of fire and law enforcement stations, critical energy and water infrastructure. (NV)
- Voluntarily contributed vulnerability assessment or other security-sensitive information a public office receives is not a public record. (OH)
- Vulnerability assessments of critical assets in water and wastewater systems made by public utilities or state environmental agencies. Vulnerability assessments of government facilities and public improvements. (OK)
- Vulnerability to terrorism assessments of critical infrastructure. (TX)
- Vulnerability assessments, operation and security manuals for public buildings. (VT)
- Vulnerability assessments…operational, procedural, transportation, and tactical planning or training manuals, staff meeting minutes or other records. (VA)
- Vulnerability assessments and underlying data…Vulnerability assessments of local schools. Vulnerability and security assessments/plans involving water supply. (WA)
- Specific or unique vulnerability assessments, specific or unique response plans, data, databases, and inventories of goods or materials assembled to respond to terrorist acts. (WV)

Exemptions for Building Plans (9)

- Government building plans and drawings. (CT)
- Blueprints, schematic drawings, diagrams, operational manuals and other security records for buildings where hazardous materials are used or stored…Buildings or structures operated by the State or any of its political subdivisions, revealing safety and support systems, surveillance techniques, alarm or security systems or technologies, operational and evacuation plans or protocols, or personnel deployments. (DE)
- Building plans, blueprints, schematic drawings, and diagrams which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency…Building plans for attractions and recreation facility, entertainment or resort complex, industrial complex, retail and service development, office development, or hotel or motel development, which documents are held by an agency. Does not apply to comprehensive plans or site plans, approved under local land development regulations, local zoning regulations, or development-of-regional-impact review. (FL)
- Any plan, blueprint, or other material which if made public could compromise security against sabotage, criminal, or terrorist acts. (GA)
- Buildings, facilities, infrastructures and systems records held by a public agency. Sport stadiums, convention centers, and all

government owned, operated, or occupied buildings (Architects' plans, engineers' technical submissions, construction-related technical documents for projects). (ID)
- Building and public facility plans, drawings, specifications for buildings, facilities. (KA)
- Structural plans of public property. (MO)
- Building plans. (VT)
- Building plans, etc. that reveal the building's or structure's internal layout, specific location, life and safety and support systems, structural elements, surveillance techniques, alarms, security systems or technologies…Building Plans, etc. for structures where hazardous materials are stored. Building plans, etc for arenas, stadiums and waste and water systems. (WY)

Exemptions for Infrastructure Information (14)
- State infrastructure…detailed description or evaluation of systems, facilities, or infrastructure in the state. (AK)
- Infrastructure risk assessments done for federal government. Emphasis on drinking water systems. (AZ)
- Arenas, stadiums. (DE)
- Critical asset protection plan and information gathered in producing the plan. Includes, but is not limited to, surveys, lists, maps, or photographs. (IA)
- Infrastructure vulnerabilities: includes IT, communication, electrical, fire suppression, ventilation, water, wastewater, sewage, and gas systems; public building vulnerabilities -- detailed drawings, schematics, maps, or specifications of structural elements, floor plans, and operating, utility, or security systems. The exact physical location of hazardous chemical, radiological, or biological materials. (KY)
- (Oil and gas) pipeline security information: physical security information, proprietary information, vulnerability assessments, operational plans and analysis of such information, and internal security information. Any such records in the custody of the office of conservation. (LA)
- Building plans and security information for airports and other mass transit facilities, bridges, tunnels, emergency response facilities or structures, buildings where hazardous materials are stored, arenas, stadiums, waste and water systems, and any other building, structure, or facility. (MD)
- Any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation or other infrastructure. (MA)
- Infrastructure records, security and personal safety information, safety of public and private buildings. (MI)
- Infrastructure information voluntarily submitted to any public governmental body for safety. (MO)
- Infrastructure, including airports, the Capitol Complex, dams, gaming establishments, governmental buildings, highways, hotels, information technology infrastructure, lakes, places of worship, power lines, public buildings, public utilities, reservoirs, rivers and their tributaries, and water facilities. (NV)
- Critical infrastructure security system plans. (ND)
- Security or infrastructure records, including vulnerability assessments. (OH)
- Critical infrastructure building plans…engineering or architectural records. (VA)

Exemptions Involving Water Systems (6)
- Records, including analyses, investigations, studies, reports, recommendations, requests for proposals, drawings, diagrams, blueprints, and plans, containing information relating to security for any public water system. (AR)
- Water company vulnerability assessments. (CT)

- Waste and water systems, electric transmission lines and substations, high-pressure natural gas pipelines and compressor stations.
- Water treatment facilities.
- The location of community drinking water wells and surface water intakes; infrastructure records that disclose the configuration of critical systems such as communication, electrical, ventilation, water, and wastewater systems. (IN)
- Sewer or wastewater treatment systems, facilities or equipment. (KA)

Exemptions Involving Utilities (3)

- Maps and other records regarding the location or security of a utility's generation, transmission, distribution, storage, gathering, treatment, or switching facilities. (ID)
- Utility, including fuel and communications facilities, plans, drawings. (KA)
- Utility records, plans reflecting structural or operational vulnerabilities, or that would permit unlawful disruption to, or interference with, the services provided. (TN)

Exemption Involving Telecommunications Networks (1)

Facilities and switching equipment. Response procedures or plans prepared to prevent or respond to emergency situations. (DE)

Exemptions Involving Transportation (6)

- Plans for mass transit facilities, bridges, tunnels, emergency response facilities or structures. (DE)
- Airport facilities…Security portions of system safety programs, investigation reports, surveys, schedules, lists, data, or information compiled, collected, or prepared by or for the Regional Transportation Authority. (ID)
- Detailed drawings, specifications of any building or facility of a public airport. (IN)
- Transportation systems. (KA)
- Public and private port security plans, vessel or fleet security plans, port or facility vulnerability assessments, security and safety plans, or other information related to security plans, procedures, or programs for facilities or vessels shall not be deemed a public record. (LA)
- Personnel deployments for airports and other mass transit facilities, bridges, tunnels, emergency response facilities. (WY)

State Laws and Cybersecurity

Most states took no legislative action in the area of cybersecurity, or in any way related to technological information contained in public records. New laws in the 22 states that did act, largely focus on protecting government computer and communications systems.

For the most part, the new laws cover information that would normally be considered sensitive and protected by rule or policy, such as access codes, passwords, ID numbers, and similar routine security mechanisms. Several states protected information about systems that serve critical services such as energy, water and communications.

Connecticut, in safeguarding information on "standards, procedures, processes, software and codes" provided that the information exempted must be "not otherwise available to the public." Maine, on the other hand, exempted information related to design, architecture, encryption, technology infrastructure and systems, and any other information that might jeopardize the integrity, availability, confidentiality, or corrupt the data in IT systems.

Illinois established an exemption for geographic systems information and three states, North Dakota, Oregon and Delaware, specifically identified telecommunications systems.

At the same time, in a number of states, cybersecurity also became one of the areas of attention for law enforcement personnel in fusion centers that were set up. Several of these intelligence/information centers have enlisted the participation of computer industry experts.

There are multiple aspects to the cybersecurity equation – prevent spying, protect systems that control critical infrastructure, and avert the interruption of critical services, including the computer networks themselves.

To most of the threats, the solutions are widely seen to be overcoming technical challenges that require an open source, information sharing approach.

Cybersecurity is also an area where the private and public systems are interdependent, where the primary protective measures and response actions must span geographic and public-private sector boundaries, and where resiliency – the ability to come back quickly – may be more critical than protection.

We need only think back a few years to the electrical grid failure which paralyzed the Northeast, shutting down communications systems, crippling financial networks, hampering emergency response operations, to understand the interdependencies.

Or extrapolate just a bit on the cyber attack on Estonia earlier this year when someone – Russia is the likely suspect – sought to shut down the government and that nation's banking system by flooding their computer systems with a form of spam. For a few hours, it worked.

This, more than any other factor, may explain the limited and narrowly-focused legislative response by the states. As with several of the areas we will be discussing, new laws may be needed far less than a new culture of cooperation and information sharing.

"Information is the coin of the economic realm, and information that is used is information that moves about. Winners have the most information in play," risk services consultant Daniel Greer told the House Homeland Security subcommittee in April.

"On the Internet, every sociopath is your next door neighbor," he said. "You can never retreat to a safe neighborhood. Your ability to defend depends on your ability to know what the current threat profile is, both generally to all and specifically to yourself."

O. Sami Saydjari, president of Professionals for Cyber Defense, told that same subcommittee that what is needed is a Manhattan Project-like program that is not shrouded in secrecy. "Doing so would be unnecessary and deleterious to the program goals. The nation's best minds must work on this difficult problem, and many of them are to be found outside government in academia and industry. Excluding those minds by making the program secret would only decrease our chances of success…A design that counts on its own secrecy to succeed isn't a robust design at all: we all know how fleeting secrets can be."

The role of the states would logically seem to be in ensuring information partnerships that bring together those who need work together at the local, state levels and regional levels.

It may be necessary to shield some information as a deterrent, but the greater challenge will be to foster the sharing of intelligence and technical information with those who can use it to make us more secure.

No Specific Statutory Provisions (29)

- Alaska
- Arizona
- California
- Colorado
- District of Columbia

- Florida
- Hawaii
- Idaho
- Iowa
- Louisiana
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Montana
- New Hampshire
- New Jersey
- New Mexico
- Ohio
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Utah
- Vermont
- Virginia
- Wisconsin

Exemptions for Cybersecurity Information (22)

- Measures, procedures, instructions, or related data used to cause a computer or a computer system or network, including telecommunication networks or applications thereon, to perform security functions, including, but not limited to, passwords, personal identification numbers, transaction authorization mechanisms, and other means of preventing access to computers, computer systems or networks, or any data residing therein. (AL)
- Measures and procedures related to computer and computer network security functions, including, but not limited to, passwords, personal identification numbers, transaction authorization mechanisms, and other means of preventing access to computers. (AR)
- Records of standards, procedures, processes, software and codes, not otherwise available to the public. (CT)
- Telecommunications networks facilities and switching equipment. (DE)
- Security plans and vulnerability assessments for…technology infrastructure. (GA)
- Computer geographic system information. Maps showing the location of utilities. (IL)
- Infrastructure records that disclose the configuration of critical systems such as communication, electrical, ventilation, water, and wastewater systems. (IN)
- Systems, facilities or equipment used in the production, transmission or distribution of energy, water or communications services. (KA)
- Infrastructure records that expose a vulnerability referred to in this subparagraph through the disclosure of the location, configuration, or security of critical systems, including information technology and communications. (KY)
- The architecture, design, access authentication, encryption or security of information technology infrastructure and systems…Information technology systems. Records describing security and information technology system plans and security procedures; and…data integrity. Records or information that will jeopardize the security, availability, confidentiality, integrity of, or corrupt the data residing in, information technology systems including records describing the architecture, data model, design, access, encryption or user authentication of information technology systems and infrastructure, including security features for preventing duplication, alteration and substitution of licenses and identification cards. (ME)
- Computer and telecommunications system or network information. (MO)

- Property; computer or communications network schema, passwords, and user identification names, guard schedules; or lock combinations. (NE)
- Records related to information technology assets, such assets encompassing both electronic information systems and infrastructures. (NY)
- Infrastructure and security of information systems, including, without limitation: (1) Access codes, passwords and programs used to ensure the security of an information system; (2) Access codes used to ensure the security of software applications; (3) Procedures and processes used to ensure the security of an information system; and (4) Plans used to reestablish security and service with respect to an information system after security has been breached or service has been interrupted… Assessments and plans that relate specifically and uniquely to the vulnerability of an information system or to the measures which will be taken to respond to such vulnerability, including, without limitation, any compiled underlying data necessary to prepare such assessments and plans…The results of tests of the security of an information system, insofar as those results reveal specific vulnerabilities relative to the information system. (NV)
- Public records do not include plans to prevent or respond to terrorist activity, to the extent such records set forth vulnerability and risk assessments, potential targets, specific tactics, or specific security or emergency procedures, the disclosure of which would jeopardize the safety…a governmental…information storage system. (NC)
- Critical infrastructure information is exempt. "Critical infrastructure "means… telecommunications centers and computers. (ND)
- Information technology of a public body or public official but only if the information specifically identifies: 1. Design or functional schematics that demonstrate the relationship or connections between devices or systems; 2. System configuration information; 3. Security monitoring and response equipment placement and configuration; 4. Specific location or placement of systems, components or devices; 5. System identification numbers, names, or connecting circuits. (OK)
- Telecommunication systems, including cellular, wireless or radio systems. Data transmissions by whatever means provided. (OR)
- Information is confidential if the information…relates to the details of the encryption codes or security keys for a public communications system…Information, including access codes and passwords, in the possession of a governmental entity that relates to the specifications, operating procedures, or location of a security system used to protect public or private property. (TX)
- Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities. (WA)
- Computing, telecommunications and network security records, passwords, security codes or programs used to respond to or plan against acts of terrorism which may be the subject of a terrorist act…Architectural or infrastructure designs, maps and plans that show computing and telecommunications infrastructure. (WV)
- Information regarding design, elements and components, and location of state IT security systems and physical security systems. (WY)

State Laws and Political Structure Modification

The most common legislation in this category provided for increased information sharing, usually, but not exclusively with the federal government. Sixteen states adopted the new laws to create exemptions from state open records laws for sensitive information received from federal officials. In several cases, the legislation also authorized the sharing of sensitive information among agencies, breaking down state stovepipes.

Texas, for example, provided that the head of a government agency could share otherwise confidential information with disaster task forces. Florida added language that allowed the inclusion of private entities in the information sharing network. Iowa highlighted the driving force behind its information withholding, authorizing exemptions as needed to avoid the loss of federal funds, but "only to the degree necessary."

Ten states created homeland security units or similar new entities to prepare for possible terrorist attacks and eight others legislated operational changes such as HAZMAT incident reporting, commissioning a ports security report, and expanding emergency powers.

Fourteen states made changes in meetings or records procedures to safeguard information on security preparations, with a number clearly struggling with concerns about the public's right to know as they restricted the availability of information.

Iowa lawmakers decided that lists of critical assets could be inspected but not copied. Iowa also mandated roll call votes by governmental bodies before closing meetings to discuss sensitive security information, as did Ohio. And Iowa said that closed discussions should be limited to matters involving critical infrastructure. It required that detailed minutes and a taped record of the closed meeting be kept; those records to be made available in the event of litigation. New Hampshire also mandated that minutes be kept but sealed until there is no longer a threat related to the matter discussed. Texas also required a full record be kept.

Oregon provided that journalists could attend any closed meeting on security issues provided they do not publish what they observe. This unusual step of was intended to allow reporters to challenge the meeting's closure in court, if they observe any discussion or action that goes beyond the legal bounds for closure.

And Texas, aware of the importance of communications in emergency situations, permitted the monitoring of emergency communications by "bona fide" local news media.

Nevada wasn't prepared to say that "restricted" information was totally off limits, but it clearly felt a need to impose some limits on who might access the information. So lawmakers set up a request procedure that requires the requester to identify himself and provide a statement of purpose. If the request is approved, a government official must be present to observe while any restricted document is reviewed.

No Statutory Provisions (15)

- Connecticut
- District of Columbia
- Hawaii
- Kansas
- Kentucky
- Maine
- Mississippi
- Nebraska
- New Mexico
- New York
- New Jersey
- North Carolina
- North Dakota
- South Dakota
- Vermont

Specific Information Sharing Provision (16)

- Provides for federal information sharing and protection of federal documents. (DE)
- Provides for information sharing, maintaining confidentiality of information, from both other governmental and private sources. (FL)
- Exempts records that are specifically required by the federal government to be kept confidential. (GA)
- Exempts any public record also exempt by federal or regulations. (ID)
- Exempts information specifically prohibited from disclosure by federal or rules and regulations adopted under federal law. (IL)
- Exempts records required to be kept confidential by federal law. (IN)
- Allows for an exemption if the loss of federal funds is threatened, but only to the degree necessary. (IA)
- Exempts records received by any public body from the federal government or records may be kept confidential to the extent required by federal law. (OK)
- Exempts records, reports, opinions, information, and statements required to be kept confidential by federal law or regulation. (RI)
- Exempts records required to be kept confidential by federal statute or regulation as a condition for the receipt of federal funds or for participation in a federally funded program. (TN)
- Allows the head of a government unit to disclose confidential information during a "state of disaster" to a task force as needed…Exempts information, other than financial, prepared for a US agency report, or related to terrorism, that is confidential under federal law or as part of an information sharing program. (TX)
- Exempts records not subject to public disclosure under federal law that are shared with the state. (WA)
- Exempts national security records shared by federal agencies. (WV)
- Exempts any record specifically exempted from disclosure by federal law. (WI)
- Exempts information that is exempt under federal law. (WY)
- Information provided by the federal government, or another government, and designated in writing as confidential. (UT)

New Entities (10)

- Created a state Department of Homeland Security but left its records subject to existing state and federal laws. In 2005, included a meetings exemption for discussion of homeland security plans. (AL)
- Created an emergency response commission and empowered it to adopt modification to the administrative procedures act as it related to the handling of public information requests, implementing chemical emergency planning and preparedness and right to know programs, and reporting on toxic releases. (AZ)
- Created an office of preparedness, security, and fire safety to develop terrorist preparedness plans and for the sharing and protection of specialized details of government information on security arrangements and investigations. (CO)
- Established a counterterrorism and security council; other agencies may consult with it on whether to disclose sensitive records. (IN)
- Established a homeland security and emergency management division. (IA)
- Created Governor's Office of Homeland Security and Emergency Preparedness. (LA)
- Established the Maryland Security Council. (MD)
- Established a division of homeland security. (OH)
- Created Oklahoma Office of Homeland Security. (OK)

- Established regional emergency response task forces. (PA)

Operational Changes (8)

- Created a HAZMAT incident or accident reporting system. (AR)
- Governor and the state public health department empowered to declare a public health emergency in event of bioterrorism attack. (GA)
- Directed those who store hazardous waste to analyze security measures and implement improvements as necessary. The analyses must be submitted to the state, but remain confidential. (MD)
- Governor gets expanded emergency powers in event of disaster, natural or man-made, or an act of terrorism. (MO)
- Officials directed to designate respective records as essential for emergencies and reestablishment of normal government operations. Then provide for their security. (MT)
- Directed Department of Natural Resources to set up confidential security plan for ports. (OH)
- Directs governor to prepare appropriate disaster plans and in doing so to withhold private information voluntarily submitted… Requires the Department of Emergency Management, working with local emergency agencies, to provide an annual report to the legislature that is confidential. (VA)
- "Omnibus Terrorism Protection and Homeland Defense Act of 2002" criminalizes aid to a terrorist or terrorist organizations, increases penalties for various terrorist activity and increases the government's power to conduct roving wiretaps. (SC)

Procedural Changes (13)

- Legislative meetings can be closed for "security" reasons…Legislative committee assignments can be conditioned on confidentiality agreements. (AK)
- Water distribution boards may meet in executive session. (AR)
- Makes it a crime for officials to disclose information discussed in closed meeting. (CA)
- Provided that lists of critical assets may be viewed but not copied…Allows closed meetings to discuss sensitive information involving airports, cities, public utilities and water districts but only after a public vote. Detailed minutes and taped record must be kept, with court to review if closure is challenged. (IA)
- Permits public bodies to close meetings when receiving security briefings and reports. However, all financial issues related to security matters must be made open to the public. (MN)
- May close meetings, records and votes for security reasons but procurement records must remain open. Board/agency must affirmatively state in writing that disclosure would impair their ability to protect the security and that public interest in non-disclosure outweighs the public interest in disclosure…Agency must review records submitted voluntarily within 90 days and return if information is not needed for security purposes. (MO)
- Gave governor the authority, by executive order, to withhold release of specific security related records. Provided criminal penalties for unauthorized release of those documents. Set up a request procedure that requires identification of the requester asking to see a restricted document, including providing a statement of purpose. A government official must be present to observe while a restricted document is being reviewed. (NV)
- Allows for closed meetings to consider emergency issues related to terrorism. Must keep minutes, but sensitive portions can be withheld until threat no longer exists. (NH)

- Board must hold roll call vote to go into executive session to discuss security and emergency response information. (OH)
- May close meeting to discuss those security issues. Must keep a full record. (TX)
- "Bona fide local news media" may monitor emergency communications. (TX)
- Permits journalists to attend but not to publish what they observe at closed meetings to discuss security issues (this allows reporters to challenge in court any inappropriate use of the executive session exemption.). (OR)
- Government bodies may hold an executive session or close records pertaining to the discussion of terrorist plans or protection against terrorist attacks. (OK)

State Laws and First Response

The exemptions written by states dealing with first response efforts are primarily designed to protect information on planning and procedures for responding to a terrorist attack. They cover everything from the emergency protocols to sheltering.

The language of some of the laws might be interpreted in ways that could hinder effective response because it withholds from the public information such as evacuation procedures and shelter details that people will need in any emergency or natural disaster.

Some of the exemptions also raise questions about the extent of public's knowledge about emergency procedures, and their degree of confidence: Will citizens make correct, instinctive responses in a post-attack situation if vital response information is withheld until after the fact? And now, in advance of any possible attack, will they press for and support needed changes and resources?

Ohio law makes information on trauma center capacity confidential. Is it reasonable to assume that government, on its own, in the absence of pressure from an informed public, will act to make the changes needed to increase center capacity where needed?

Another example: Virginia exempts school safety audits. That's information I'd want and demand as a parent concerned about my child's welfare. And it is information I'd use as a parent to force improvements, if needed.

By way of contrast, Arizona created a new agency to establish procedures for handling information the public must have and to establish right to know reporting requirements.

First Response Laws

No Statutory Provisions (21)

- Alabama
- Alaska
- Arkansas
- California
- Georgia
- Hawaii
- Kentucky
- Louisiana
- Maine
- Minnesota
- Mississippi
- Montana
- Nebraska
- New Mexico
- New York
- Oregon
- Rhode Island
- South Carolina
- South Dakota
- Vermont
- Wisconsin

Exemptions for Emergency Response Plans, Records (28)

- Protocols and procedures concerning the prevention of, preparation for, response to, and recovery from any terrorist threat, ter-

rorist act, or other terrorist-related activity; or terrorist training activity. (CO)
- Government training manuals on emergency plans or security equipment; emergency plans and emergency recovery or response plans. (CT)
- Response procedures or plans prepared to prevent or respond to emergency situations. Records prepared to prevent or respond to emergency situations. (DE)
- Any specific response plan. (DC)
- Emergency evacuation plans; sheltering arrangements; manuals for security personnel, emergency equipment, or security training. Hospital Security systems or plans, emergency evacuation transportation, sheltering arrangements, emergency equipment. (FL)
- Emergency evacuation, escape or other emergency response plans. (ID)
- Plans designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations. (IL)
- Emergency contact information of emergency responders and volunteers. (IN)
- Emergency preparedness information developed and maintained by a government body for the protection of governmental employees, visitors to the government body, persons in the care, custody, or under the control of the government body, or property under the jurisdiction of the government body. (IA)
- Emergency records, security information and procedures of public agencies. (KA)
- Response procedures or plans prepared to prevent or respond to emergency situations, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures, or specific security procedures. Records prepared to prevent or respond to emergency situations identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities, or laboratories. (MD)
- Security measures, emergency preparedness. (MA)
- Emergency response plans, risk planning documents, threat assessments, and domestic preparedness strategies. (MI)
- Operational guidelines and policies developed, adopted, or maintained by any public agency responsible for…first response. (MO)
- Document, record or other information prepared and maintained for the purpose of preventing or responding to an act of terrorism, including: documents, records or other items of information which may reveal the details of a specific emergency response plan or other tactical operations by a response agency and any training relating to such emergency response plans or tactical operations…Resort hotel emergency response plans that include:

(a) a drawing or map of the layout of all areas within the building or buildings and grounds that constitute a part of the resort hotel and its support systems and a brief description of the purpose or use for each area; (b) a drawing or description of the internal and external access routes; (c) the location and inventory of emergency response equipment and resources; (d) the location of any unusually hazardous substances; (e) the name and telephone number of the emergency response coordinator for the resort hotel; (f) the location of one or more site emergency response command posts; (g) a description of any special equipment needed to respond to an emergency at the resort hotel; (h) an evacuation plan; (i) a description of any public health or safety hazards present on the site; (j) any other information requested by a local fire department or local law enforcement agency whose jurisdiction includes the area in which the resort hotel is located or by the Division of Emergency Management. (NV)

- Records pertaining to the preparation for and the carrying out of all emergency functions, including training…developed by local or state safety officials that are directly intended to thwart a deliberate act that is intended to result in widespread or severe damage to property or widespread injury or loss of life. (NH)
- Emergency or security information or procedures for buildings or facilities. (NJ)
- Specific security or emergency procedures plans. Emergency response plans adopted by a constituent institution of The University of North Carolina, a community college, or a public hospital. (NC)
- A security system plan kept by a public entity. "Security system plan" includes…. emergency evacuation plans. (ND)
- Deployment plans of law enforcement or emergency response personnel; trauma center reports on preparedness and capacity to respond to disasters, mass casualties, and bioterrorism. Provides for information sharing with appropriate first responders. (OH)
- Records including details for response, remediation after act of terrorism. (OK)
- Contingency plans of law enforcement agencies prepared to respond to any violent incident, bomb threat, ongoing act of violence at a school or business, ongoing act of violence at a place of public gathering, threat involving a weapon of mass destruction, or terrorist incident. (TN)
- Staffing requirements of an emergency response provider, including a law enforcement agency, a fire-fighting agency, or an emergency services agency; tactical plan of the provider. Lists of pager or telephone numbers, including mobile and cellular telephone numbers, of the provider. (TX)
- Division of Emergency Services and Homeland Security records of emergency plans or programs. (UT)
- School safety audits and school crisis, emergency management, and medical emergency response plans (the local school board retains authority to withhold or limit the release of any security plans). (VA)
- Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, including specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility. Emergency/escape response plans for detention facilities. (WA)
- Those portions of records containing… deployment plans of law enforcement or emergency response personnel. (WV)
- Specific tactics, emergency procedures or security procedures. Personnel deployments for airports and other mass transit facilities, bridges, tunnels, emergency response facilities or structures, buildings where hazardous materials are stored, arenas, stadiums and waste and water systems. (WY)

New Agencies (2)

- Created an emergency response commission to establish procedures for handling public information requests, community right-to-know program reporting requirements, release reporting requirements. (AZ)
- Created regional counterterrorism task forces, including first responders to develop response plans. (PA)

State Laws and Public Health

Only 16 states enacted new legislation in the area of Public Health, and half of those did so to safeguard prevention or response plans. Florida, in exempting emergency response plans, also called for appropriate information sharing, a concerned that also surfaced in legislation approved in other states. Louisiana approved a new law that pro-

vided for the tracking and sharing of health emergency information while also providing penalties for breaching confidentiality.

New laws were written in four states to protect records that listed the locations of hazardous materials, although Texas noted that some of this information is already public. It limited the non-disclosure to "unpublished information."

Only one state, Utah, offered special records protection for risk assessments in the public health area. And only two dealt with health investigations. Missouri said public health officials could keep secret some information about their investigations and Ohio mandated that names of people and businesses under investigation be kept confidential until a case is completed.

Two states made structural changes related to public health, with Arizona setting up an emergency response commission and Georgia giving the governor new power to declare a health emergency if there is a bioterrorism attack.

The relative inactivity in this area may come from recognition that advance public knowledge is critical and that open communication is vital to rapid and effective response to public health concerns. It may also be an acknowledgement that the federal government has an existing oversight role on biomedical issues and disease prevention. Moreover, Congress passed a sweeping "Public Health Security and Bioterrorism Preparedness and Response Act of 2002," shortly after 9/11.

Also, there is considerable controversy over the desirability of restrictions on information sharing within the scientific and medical communities. The National Academies said in a 2004 report, *Seeking Security; Pathogens, Open Access and Genomic Data Bases,* that there should be no change in current policies that allow scientists and the public unrestricted access to genome data on microbial pathogens. Access, it concluded, improves the nation's ability to fight both bioterrorism and naturally occurring infectious diseases.

Public Health Laws

No Specific Statutory Provisions (33)

- Alabama
- Arkansas
- California
- Hawaii
- Idaho
- Illinois
- Indiana
- Kansas
- Kentucky
- Maine
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Vermont
- Washington
- Wisconsin

Public Health Records Exemptions (16)

- Records that could reasonably be expected to endanger the life or physical safety of an individual or to present a real and sub-

stantial risk to the public health and welfare. (AK)
- Communicable disease reports and similar records are deemed confidential but can be released to FBI, federal law enforcement agencies or prosecutors to investigate or prosecute bioterrorism. (CO)
- Confidential prevention plans filed with Health Department. (CT)
- Records that identify and locate pharmaceutical caches, or security information about medical facilities, storage. (DE)
- Comprehensive emergency response plan, including hospitals, are deemed confidential, with an information sharing provision. (FL)
- Plans for responses to bioterrorism, and proposed or actual plans and responses involving the National Pharmacy Stockpile…Notices sent to the state health department regarding certain illnesses or unusual prescription trends. (GA)
- Medical examiner records and reports, including preliminary reports, investigative reports, and autopsy reports. (IA)
- Established procedures to detect, track, and share information on public health emergencies focusing on the immediate reporting of incidents. Provides penalties for unauthorized disclosure of confidential information. (LA)
- Information in the newly established Biological Agents Registry program. Also records prepared to prevent or respond to emergency situations identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities, or laboratories. (MD)
- Meetings, records and votes on operational guidelines and policies of public health agency for first response…Information reported and evaluations of the reports to trauma centers are not public record…State public health officials may keep secret some information about health investigations of the suspected origins of bioterrorism attacks. (MO)
- The identities of people and businesses under investigation in bioterrorism cases, until the case is completed…Information reported by trauma centers to the public health council on preparedness and capacity to respond to disasters, mass casualties, and bioterrorism, and evaluations of those reports. (OH)
- Unpublished information about the location of a chemical, biological agent, toxin, or radioactive material and about any potential vaccine or to a device that detects biological agents or toxins. (TX)
- Information regarding food security or risk, and vulnerability assessments performed by the Department of Agriculture and Food. (UT)
- Records of the State Health Commissioner relating to the health of persons under quarantine. (VA)
- Records assembled, prepared or maintained to prevent, mitigate or respond to terrorist acts or the threat of terrorist acts, the public disclosure of which threaten the public safety or the public health. (WV)
- Records prepared to prevent or respond to terrorist attacks or other security threats identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities or laboratories established, maintained, or regulated by the state or any of its political subdivisions. (WY)

New Agency or Plan (3)
- Established an emergency response commission including the Department of Health Services. (AZ)
- Mandated a response plan to deal with threats of bioterrorism. (DC)

- Gave the governor the power to declare a public health emergency in bioterrorism cases and provided for notification to the state health department of certain illnesses or unusual prescription trends. (GA)

State Laws and Terror Investigations

State and local law enforcement agencies have historically declined to disclose sensitive investigative and intelligence information, a position supported by common law, state public records law and local ordinance. That tradition and confidence in law enforcement's existing authority to withhold intelligence information likely explains why fewer than half of the states took any action in this area after 9/11.

Most states that did write new law did little more than codify or update traditional law enforcement exemptions, such as exemptions for investigatory reports and intelligence files and reports and information related to sources and methods and surveillance. Illinois did expand an exemption for investigation reports to include a regional transportation authority.

The most specific new law involving investigations may the one in Texas, which makes confidential information that is collected, assembled or maintained by emergency response providers to prevent, detect, respond to, or investigate an act of terrorism.

Five states adopted information sharing legislation focused on terrorism investigations.
Only two states wrote legislation in the area of surveillance programs.

Terror Investigation Laws

No Specific Statutory Provisions (28)

- Alabama
- Arizona
- Arkansas
- Connecticut
- Hawaii
- Idaho
- Kansas
- Kentucky
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Jersey
- New Mexico
- North Carolina
- North Dakota
- Rhode Island
- South Dakota
- Tennessee
- Utah
- Vermont
- Washington
- Wyoming
- Wisconsin

Exemptions for Intelligence Files and Information (3)

- Law enforcement intelligence files. (DE)
- Terrorist intelligence information. (LA)
- Reports, records that contain intelligence and investigative information; information on investigative techniques and procedures not known by the general public. (ME)

Exemptions for Surveillance (2)

- Information on surveillance techniques and procedures or personnel. (FL)
- Expanded pen registers and other wiretapping provisions. (MD)

Exemptions for Investigation Reports (10)

- Records of state and local security complaints and investigations. But requires disclosure of non-sensitive incident infor-

mation to victims and insurers, and public disclosure of basic incident information, including identity information on those arrested, and details of arrest, and basic incident information. (CA)
- Investigation reports prepared by or for the Regional Transportation Authority. (IL)
- Investigatory records and intelligence and threat assessments. (IN)
- Medical examiner records; preliminary, investigative and autopsy reports. (IA)
- Law enforcement investigative information, information on confidential sources, and methods of investigation. (NY)
- Any record assembled, prepared, or maintained by a public office or public body to prevent, mitigate, or respond to acts of terrorism. (OH)
- Investigative evidence of a plan or scheme to commit an act of terrorism and of an act of terrorism that has already been committed. (OK)
- Makes confidential information that is collected, assembled, or maintained by to prevent, detect, respond to, or investigate an act of terrorism. (TX)
- Records assembled, prepared or maintained to prevent, mitigate or respond to terrorist acts or the threat of terrorist acts. (WV)

Exemptions for Sources and Methods (3)
- Information identifying confidential sources or disclosing confidential surveillance or investigations or investigative or prosecution material. (GA)
- Investigatory records that identify confidential sources and their information, or reveals investigative techniques and procedures not generally known outside the government, or endangering safety of law-enforcement personnel. (DC)
- Law enforcement records that identify informants, disclose investigatory techniques, and reveal contents of wiretaps or other surveillance. (SC)

Provisions for Information Sharing (5)
- Allows for information sharing of specialized details of security arrangements or investigations. Also for communicable disease reports by a new office of preparedness, security and fire safety. Requires disclosure of records on the funding of security arrangements and investigations. (CO)
- Allows for release of information from investigative files on a limited basis to persons whose health and safety may be affected. (NH)
- Provides for law enforcement information sharing. (VA)
- Intelligence information and investigative records dealing with terrorist acts or threats may be shared with federal and international law-enforcement agencies. (WV)
- Specific intelligence information and specific investigative records shared by federal and international law enforcement agencies. (OH)

Other (2)
- Expanded the exemption for security records of public safety agencies to other public bodies and includes meetings. (OR)
- Permits closure of regional counterterrorism task force meetings called to discuss sensitive law enforcement, threat assessment, or facility safety information. (PA)

Protecting Our Security – On All Fronts

When victory in our nation's third great war was finally in sight, though still a long way off, President Franklin D. Roosevelt used his 11th State of the Union address to urge the country to turn its thinking from the demands of wartime security to longer term concerns – to the nation's "economic security, social security and moral security."

Only when we have established each of these, he said, will we have gained true and total national security.

Today, our nation is engaged in a self-declared "war" against terrorism, a very different kind of conflict involving hostile ideologies that transcend nation-state boundaries. The weapons and methods are unconventional. It is a war, as we saw on Sept. 11, 2001, that involves using our assets as weapons against us.

The governmental response to this new threat, especially at the federal level, has followed a more traditional path. It has at times created its own threats to individual security – the loss of our civil liberties and rights. And it has endangered another form of security critical to our democratic system and our way of life – the public's right to know.

States Moved More Cautiously than Washington

Many of our states have stronger open records and open meetings traditions than those found in Washington, and so it is not surprising that these states were more cautious than the federal government as they acted following 9/11 to protect information that might be useful to terrorists. In drafting safeguarding legislation, many state lawmakers tried to anticipate the collateral consequences. In doing so, they set standards for the withholding of information, establishing criteria designed to avoid unnecessary secrecy. Sometimes lawmakers put in critical caveats or disclaimers, hoping to insure that security concerns would not overwhelm other public health, welfare and accountability concerns.

For example, North Carolina provided that the new exemptions did not cover budget authorizations and expenditures used to implement public security plans and security measures, or for the construction, renovation, or repair of public buildings and infrastructure facilities.

Similarly, Missouri, in protecting operational guidelines and policies for first responders, made it clear that it was not exempting records on expenditures, purchases, or contracts – areas critical to maintaining the accountability of the agencies involved.

Missouri also added an important caveat in setting out a protection for security-related information that is voluntarily submitted. It said the exemption does not apply to information already in the public record, thus preventing agencies and private entities from using a security exemption to seal nonsensitive information they would prefer the public not know about.

West Virginia, in providing for the withholding of information on terrorism security, declared that the new law did not create an exemption for information related to any immediate threat to public health or safety that is unrelated to a terrorist act or the threat.

Kentucky, after laying out a long list of exempted information, added this important qualifier: "Nothing in this paragraph shall affect the obligations of a public agency with respect to disclosure and availability of public records under state environmental, health, and safety programs."

Iowa sought to balance its concerns about terrorism with the public's right to know which facilities are considered critical infrastructure by providing that lists of critical assets could be viewed but not copied

Connecticut, in exempting water company vulnerability assessments, said those documents must be maintained as separate and discrete from other records about the facilities that the public is entitled to see.

Some states presented their security-based exemptions as a last option.

Oklahoma exempted certain technology information but "only if" that disclosure revealed such sensitive information as functional schematics and system configuration.

Similarly, Maryland provided that inspection of sensitive records could be denied "only to the extent" that disclosure would jeopardize security or facilitate the planning of a terrorist attack or endanger the life or safety of an individual. At a minimum, that language suggests a need to carefully review individual documents and redact sensitive information, rather than broadly withhold records.

Tennessee said its new exemptions should not be construed by non-affected agencies to limit access to their public records.

Virginia said its exemptions should not be read to prohibit disclosure of information relating to the structural or environmental soundness of any building, nor to prevent disclosure of information in connection with an inquiry into building performance after it has been subjected to fire, explosion, natural disaster or other catastrophic event.

Ohio insisted that its new law safeguarding vulnerability assessment information should not be construed to allow the owner or operator of chemical facility to withhold information the public is entitled to review under other state or federal laws.

Setting the Bar for Non-Disclosure Decisions

In the wake of 9/11, Florida and a few other states adopted specific, narrow statutory exemptions to their public records and meetings laws. Most, however, exempted categories of information, an approach consistent with their existing records laws. In doing so, they all but universally provided qualifying language that reflected concerns about the new restrictions on the public's right to know. These new laws set out standards or criteria for officials to meet in making non-disclosure decisions.

For example, Nevada provided that the governor establish specific exemptions by executive order, and in doing so find that the each disclosure "would create a substantial likelihood of compromising, jeopardizing or otherwise threatening the public health, safety or welfare."

These standards, I believe, offer important insights into concerns that state lawmakers had in trying to find the appropriate balance between national security needs and other public interests, including everyday safety, governmental accountability, and the public's right to know.

In the language of many of the state post 9/11 statutes there is a clear indication of concern about the consequences that secrecy measures may have on other societal and democratic values. For instance, the authority to withhold information from the public in Alaska, Idaho, Illinois and Maine is granted "only to the extent" that release of information jeopardizes security interests. That language serves to narrow both the scope of the exemption and the frequency of its use.

Most states used the auxiliary verb "would" in setting the standard for non-disclosure, thus mandating that officials find that the release of information would create a clear and present danger, rather than allowing withholding of records simply when harm is theoretical or hypothetical.

Lawmakers then went further, using a variety of phrases to establish the criteria for non-disclosure. These measures provided an exemption if disclosing the information would

- Compromise security (ID & IL)
- Impair a public body's ability to protect the security or safety of persons or property. (MI)
- Create a substantial likelihood of endangering public safety or property; computer

or communications network schema, passwords, and user identification names; guard schedules; or lock combinations. (NE)
- Substantially threaten the public's safety. (NV)
- Be likely to compromise, jeopardize or otherwise threaten safety of the public. (NV)
- Jeopardize security or would create a risk to the safety of persons, property, electronic data or software. (NJ)
- Jeopardize the safety of governmental personnel or the general public or the security of any governmental facility (or) information storage system. (NC)
- Jeopardize the security of any building, structure, or facility; facilitate planning of a terrorist attack; endanger the life or physical safety of an individual.
- Threaten public safety or the public health. (WV)
- Have a substantial likelihood of threatening public safety. (WA)

In a few instances, state lawmakers chose the more conditional "could," allowing non –disclosure if there was a possibility rather than the certainty of harm. In those instances, however, they imposed a standard of reasonableness:
- Could reasonably be expected to be detrimental to the public safety or welfare. (AL)
- could reasonably be expected to interfere with the implementation or enforcement of the security plan; disclose confidential guidelines for investigations; endanger life or physical safety; present a real and substantial risk to the public health and welfare. (AK)
- Could reasonably be expected to jeopardize such employees, visitors, persons, or property. The information, if disclosed, would significantly increase the vulnerability of critical physical systems or infrastructures. (IA)
- Could reasonably be expected to interfere with the implementation or enforcement of the security plan, would disclose confidential guidelines for investigations. (AK)

Several states required subsequent reporting on records taken off the books as a result of the new authority granted to state and local agencies.

Nevada lawmakers, in giving the Department of Information Technology the authority to withhold sensitive information, insisted on full reporting of the records made confidential. The department's director must keep a list of every record and portion of a record declared confidential, and review each every other year, reporting to the legislature on whether each should remain sealed.

Missouri, in granting agencies the authority to restrict access to information about computer systems and security plans, mandated that agencies "declare in writing" that disclosure of the information would jeopardize public safety and security and that the security risk involved outweighs the public interest in disclosure.

Several states imposed sunset provisions, allowing the new laws to expire unless subsequently reenacted. Arkansas sunset a bill safeguarding water system security records and Florida and Missouri sunset bills exempting building and security plans.

Defining Terrorism

A few states put a definition with their safeguarding provisions. In doing so, they spelled out the scope of their concerns.

Maine said it was protecting against "conduct designed to cause serious bodily injury or substantial risk of bodily injury to multiple persons, substantial damage to multiple structures, or substantial physical damage sufficient to disrupt critical infrastructure;

Nevada defined terrorism as "any act that involves the use or attempted use of sabotage, coercion or violence intended to cause great bodily harm or death to the general population; or cause substantial destruction, contamination or impairment buildings, infrastructure, communications, transportation, utilities or services; any natural resource or the environment."

Kansas described terrorism as more than physical violence. It is "an act intended to intimidate or coerce a public agency or the civilian population; disrupt a utility or communications system; destroy a public building or facility."

All this legislative activity aimed at the prevention or mitigation of potential terrorist attacks raises obvious questions.

- Are we safer?
- Should we do still more?
- Have we gone too far?

Are We Safer?

The answer to the first question is that we simply do not know. That is both the nature of the threat and a consequence of the response, which has wrapped so much of what federal and state governments are doing to prevent terrorism in a shroud of secrecy.

The Congressional Research Service all but threw up its hands in its March 2007 report to Congress on implementation of critical infrastructure safeguards. CRS said it is still unclear how many critical sites there are, how many of those sites have been visited, how many have had their vulnerabilities assessed, and how many have developed and implemented buffer zone protection plans. That means, of course, that most members of Congress don't know the status of the infrastructure security measures. It also means the public is even further in the shadows.

The Department of Homeland Security has yet to report, for instance, on how many infrastructure owners (85% of the nation's critical infrastructure is privately owned) have provided security related information and how many protection plans have passed muster. The only public information comes from the DHS response to a lawsuit almost three years ago. In February 2005, the department said it had received all of 29 voluntary submissions of sensitive security information from private infrastructure owners and that it had accepted 22 of those as Critical Infrastructure Information that would be held as confidential.

The public remains very much in the dark, and in the absence of any new terrorist incident, that lack of knowledge on the efficacy of the existing programs is likely to make it difficult to gain public support for any new secrecy-expanding legislation.

Should We Do Still More?

It's doubtful you will find anyone involved with national security or anti-terrorism who would answer "no." There is, however, considerable disagreement on what is most needed, at both the national and the state levels.

After 9/11, there was a wave of legislation promulgating measures that followed a traditional risk averse approach to the safeguarding of information considered potentially useful to a terrorist intent on causing public harm. The quick and easy solution was more secrecy. But as the intelligence and law enforcement efforts leading up to 9/11 were more fully analyzed and the nature of the terrorist threat more fully assessed, the national security conversation has turned to risk assessment and the need to significantly improve information sharing across all levels of government and with appropriate private sectors.

"Poor information sharing was the single greatest failure of our government in the lead-up to the 9/11 attacks," the 9/11 Commission Vice Chair, Lee H. Hamilton told Congress in November 2005. "The failure to share information adequately, within and across federal agencies, and from federal agencies to state and local authorities, was a significant contributing factor to our government's missteps in understanding and responding to the growing threat of al Qaeda in the years before the 9/11 attacks."

In recent months, there have been several congressional hearings on information sharing problems and possibilities, focusing on shortcomings at both the federal and state levels. This conference may wish to consider how state efforts could be improved. The state laws put in place after 9/11 do not speak to the quantity or quality of information shared, or to the effectiveness of its use once received. Most do little more than permit state and local officials to treat as confidential shared information, something they are required to do anyway under federal non-disclosure agreements they must sign to get the information.

What many states have done, without specific new legislative authorization, is move to create fusion centers – multi-agency intelligence units designed to integrate information streams from national intelligence sources with those of the local and state agencies and to make sure that each of the agencies involved has the information it needs to be effective. There are now some 40 such centers across the country.

These fusion centers, described in one recent report as "maturing," are learning about a kind of intelligence far different than traditionally practiced by law enforcement, and about its very different uses. Through the working partnerships, they are developing the mutual trust that is a predicate to the sharing of information. But many state officials feel the federal government is still not sharing enough information, or the "right" information, limiting the terrorism-related work of the centers. One result is that the centers are diversifying, evolving from their initial terror intelligence missions to full-service intelligence sharing operations with increased emphasis on non-terrorist crimes.

The hearings over the spring and summer also suggest that Congress is no longer focused on expanding secrecy but rather on limiting it and expanding the sharing of information. Given these shifts in outlook, it may be appropriate, as we consider possible new state laws that make structural and procedural changes to enhance national security, to also think about measures that would enhance the prospects of genuine information sharing and permit more thoughtful risk-assessment analysis and response.

Have the states got the statutory balance right? The Heritage Foundation and the Center for Strategic and International Studies offered this caution in a December, 2004 report: "It is necessary to strike the right balances in sharing information with or withholding information from the public. Policies that are either overly neglectful or overzealous ill serve efforts to enhance homeland security."

John Gilligan, a former chief information officer for the Air Force, put national security and terrorism in a strong information sharing context at a November 2005 conference sponsored by the Information Security Oversight Office and the University of Maryland: "Today, the concern is global terrorism, an amorphous threat with no geographic or national base, with a potential for small, focused attacks. In that environment, information sharing is the best way to protect against the threat."

To which Joe Markowitz, a 24 year veteran of the CIA, added, "Running faster is better than keeping secrets." Stephen Hannestad, director of research at Maryland's College of Information Studies said, "Information sharing is and must be unstructured and dynamic. There's a far greater need for

a shift of information down to the local community, to the first providers, because the threat has changed."

Gilligan said that as a nation we must move from a risk-averse system that tries to hide information from all but the chosen few to a risk management approach that deals proactively with potential threats. That risk management approach was advocated a few days later by William P. Crowell, who headed the Markle Task Force on National Security in The Information Age. "We need to create an Information Sharing Environment that fundamentally changes the way we think about the business of national and homeland security," he told a House Intelligence subcommittee. "There are security risks not only from information falling into the wrong hands, but also from information failing to find its way into the right hands. The risk of release and sharing should be balanced with the risk of not sharing." He added, "The government's current approach to protecting classified information does not recognize this risk from failing to share. As wrenching as it is, the government must move to a risk management approach…You cannot connect dots that you cannot access." While Crowell was aiming his remarks at the federal government, its cumbersome classification system and the insularity of its intelligence community, his point has strong applicability to the states.

Do the current state laws need to be rethought? Are they the product of the same outdated, risk-averse culture of information safeguarding and classification that grew out of the Cold War? Or do they in fact provide ways to manage those risks that a broadly troubled world thrusts upon us? Do they facilitate the "need to share" and minimize the structural stovepipes that secrecy's "need to know" constructs as an impediment to effective security intelligence, planning and response?

The series of congressional hearings on information sharing and terrorism included an April field trip to Seattle where several robust local-state-national-private sector information sharing partnerships have been established. Officials involved with those fusion centers repeatedly told their representatives that federal agencies aren't sharing enough information and often make things too complicated for local officers not trained in federal intelligence ways and means.

Seattle Police Chief R. Gil Kerlikowske said the biggest impediment to information sharing is that "we remain tethered to the federally centered vision of intelligence information management… For all the stated commitment to derive intelligence requirements and priorities from the 'bottom up` – the front lines of local law enforcement – many decisions still originate from somewhere inside the beltway, and specifically within DHS and the FBI."

Kerlikowske said it is difficult for local law enforcement officials to get security clearances in a timely manner. He added that sharing is prohibited for vast categories of information unless brokered by the FBI, noting that even though he has top secret clearance, he does not have direct access "to even the most benign information." At that and the other hearings, state law enforcement officials made the point that fusion centers are rewriting the intelligence practices of local and state law enforcement agencies and creating new information sharing paradigms that may require the states to look again at their laws to make sure they facilitate rather than hinder the new approaches.

Mark Zadra, Assistant Commissioner, Florida Department of Law Enforcement, talked about that shift. "Prior to 9/11, law enforcement agencies at all levels had little need to share sensitive information with non law enforcement agencies…We had limited experience with federally classified information. Little consideration was given to sharing sensitive information outside the law enforcement community, and sharing information with the private sector was generally not done."

"The paradigm shifted after 9/11 when it became known that fourteen or more of the hijackers had lived, worked, traveled and trained across Florida while planning the atrocities they would ultimately commit. In their daily activities they left many clues that, if viewed together, may have predicted the plan and given authorities an opportunity to avert the catastrophic consequences."

The FBI's Wayne M. Murphy, Assistant Director, Directorate of Intelligence Federal Bureau of Investigation, told members of Congress in June 2007 that the government has "the capacity" to rapidly make information available to a broad set of partners. The trick, he said, is to make the sharing a benefit to the partners, not a burden.

Then he added a caution: "Most important of all, we must respect the power of that information and the impact it holds for the rights and civil liberties of the American people who have entrusted us as its stewards. That also means that we must never use 'control' as a way to deny the public access to information to which they are entitled."

Have We Gone Too Far?

A principal concern of many, including this author, focuses on the unintended consequences of secrecy – the withholding of information that restricts our knowledge of both government and private operations that have traditionally been subject to public oversight. That oversight instills an accountability that works to prevent or restrain misfeasance. In the absence of that oversight and accountability, we worry about the extent to which this new security-induced secrecy may be manipulated for reasons that have nothing to do with national security. Without openness and traditional public oversight, including media reporting, how do we ensure:

- Operational and fiscal integrity of public facilities.
- Effective regulatory review and decision-making of private facilities.
- Safety and public health protections unrelated to terrorism issues.

These elements speak to a different but very important kind of security. We call this Critical Oversight Information (COI), and we believe it must be given significant consideration in the writing of any legislation governing the public's security.

To a major degree, these oversight activities take place at the state and local levels, which may explain why the Department of Homeland Security has been largely oblivious to them in crafting its critical infrastructure and transportation security regulations, and why it so blithely talks about preempting state records laws that facilitate citizen oversight. This past spring, DHA adopted an Interim Final Rule on chemical plant security, stating that any "law, regulation, or administrative action" of a state or local government, or any action of a state court is invalid if it "conflicts with, hinders, poses an obstacle to or frustrates the purposes" of its new rule.

DHS reassured that it does not intend to preempt existing health, safety and environmental regulations "at this time" but warned that it plans to review future local and state law promulgated "under the rubric of health, safety or environmental protections" to make sure they aren't in conflict with the new DHS rule.

Then it took a further step to demonstrate that it has little concern about those issues that most concern local and state governments -- the fears of the surrounding communities. It rejected "at this time" a request to keep local communities informed about plant compliance with security requirements.

It is important to the safety of our communities and the health of our local and state governments that robust public oversight continues, whatever the security concerns. This conference would perform a special public service if it were able to offer recommendations designed to encourage and

guide approaches that would boost security without restricting Critical Oversight Information.

The last of the COI elements listed above is the public's health and safety. Unfortunately, some laws enacted in the name of national security since 9/11 have come into conflict with state laws and local regulations designed to inform and guarantee citizen safety.

Some examples:

Last January, journalists and civic activists visited more than 400 local emergency planning offices across the country, asking for a copy of the Comprehensive Emergency Response Plan – a document containing information on protections against and response to hazardous materials spills.

Community, labor and environmental organizations had fought hard in the 1980s for the public's right to know about hazardous chemicals and safety provisions in their communities. That fight resulted in the federal Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA). The act requires that each local planning office update an emergency response plan annually and then let the public know the plan is available for inspection. Yet when asked in 2007 for a copy of the plan, more than one-third of the local offices refused and another 20 percent provided only a portion of the document. Most cited national security for their refusal. Many local officials believed releasing the information violated state law adopted since 9/11.

In July, the House Subcommittee on Infrastructure Protection heard testimony on chemical plant safety. John Alexander, a safety specialist for the United Steelworkers, complained that workers, those most affected, were being kept in the dark. He made a strong argument for thoughtful separation of sensitive information, which must be kept secret for security reasons, and not so sensitive information, which could be shared to enhance the workers sense of security and personal safety measures.

"There is no question that some information should be protected from public disclosure. Which tanks contain which chemicals is an example," he said. "At the same time, a potential terrorist with knowledge of chemical engineering will almost always be able to determine what chemicals may be on the site taken as a whole. Hiding that information from the public serves no legitimate purpose."

He went on to argue that there are good reasons for the public to know about the dangers posed by nearby chemical facilities. "Community residents should have the right to know the risks they face, so they can work to reduce those risks." That, of course, was one of the purposes of the EPCRA legislation 21 years earlier.

In the summer of 2007, after the collapse of the 35-W bridge in Minneapolis, hundreds of news organizations obtained bridge inspection data from the Federal Highway Administration and reported to their readers on the condition of local bridges. Those records showed hundreds of bridges around the country in the same or worse condition as the Minneapolis bridge that collapsed.

State transportation officials in Florida and Texas initially refused requests. In fact, the Texas Department of Transportation (DOT) even said "no" to the chair of the state Senate's transportation committee. A spokesman for the department offered this explanation: "If a legislator requests such information in writing AND indicates the information is for legislative purposes, information may be provided. There must be an agreement or understanding that the requested information may not be shared further or with the public."

Virginia's Department of Transportation (VDOT) said it would continue to make available the overall inspection ratings and definitions that explain why one structure may be rated higher than another

but that it would not release specific information on which bridge components were the weakest.

VDOT officials said they are concerned that the specific information could provide terrorists with details that would permit them to inflict significant damage with relatively little effort. "We're trying to balance the public's right to know with its need to know," Malcolm T. Kerley, the department's chief engineer. "If we have a bridge in a certain structural condition, we're not going to show people where the weakest points might be."

The U.S. Department of Transportation sent a memo to state transportation agencies in August cautioning against release of detailed information, such as drawings and inspection reports, saying that concerns had been raised "that while release of such information might be useful to educate and inform the public, the information might also be used by persons planning to conduct terrorist or criminal acts."

Many government inspection records on "critical infrastructure" were taken offline after the 9/11 terrorist attacks for security reasons.

The Dallas Morning News reported this summer that the Army Corps of Engineers has not released dam inspection data since shortly after 9/11. Dams are required to be inspected every five years. The 2002 report showed there were 700 dams located near large population areas that had not been inspected for at least 10 years. Have those dams been inspected since then? Are they safe? Is government doing its job? That information is not public.

Does this sealing of information actually protect the public? Or does it put the public at greater risk? When information like this is kept secret, citizens are forced to rely on the respective agencies to properly monitor safety and inspection data and then to see that the problems are fixed once identified. We know from Hurricane Katrina in New Orleans, the Big Dig in Boston, and most recently the bridge collapse in Minneapolis that this doesn't always happen.

It is essential, as we look at the state laws that have been written since 9/11 and discuss new legislation, that we consider the relationship between national security and other forms of security and that we strive for a balance that maximizes each. We must perform a risk assessment that balances:

- The protection of infrastructure and population from terrorist acts.
- The sharing of information between public sectors and private sectors to assure both effective prevention and effective response.
- The daily and continuing health and safety of the citizenry.
- The operational integrity and efficiency of publicly run or regulated facilities.

This may involve some new techniques and information approaches, such as the applying the intelligence community's tear line approach to certain public records, finding other ways to segregate sensitive information without sealing entire documents and retraining public employees in the handling of these new form of records; creating vetted inspectors general who would assume a fiduciary oversight in areas where the public access to accountability information must preempted for security considerations; and adopting sunset provisions designed to reopen information to the public as quickly as its short-term sensitivity has passed.

Suzanne Spaulding, a consultant and former assistant general counsel for the CIA, told Congress this spring that "the danger of not classifying information that is indeed damaging to national security is well understood. What is not as widely appreciated in the national security risk of overclassification."

Similarly, I believe we need to be concerned about the tendency to over-legislate secrecy in the be-

lief it will solve our terrorism security problems. It won't, but it will put at risk other securities that are very important to our way of life.

Should There Be a Model Law?

There is still another question raised by this review and the explorations of this conference: Should there be a model law?

My own view is that a model law is neither a pragmatic nor a wise outcome. Its drafting would be a largely academic exercise that could constrain rather than advance the many valuable ideas we expect this conference to generate.

While the states generally start from the presumption that records and meetings are public unless exempted, even the quickest review of the voluminous report compiled by the Reporters Committee on existing state laws demonstrates how varied the states are in statutory approach and language. And some legislatures, like Florida's, operate within the very specific constraints set out in their constitutions. No "model law" is going to fit neatly within many, if any, existing state codes.

Nor is it likely that a single, "model" answer will emerge in all of the areas that are being explored, or that there is a single best approach for each state. The diversity of the states and of the laws adopted after 9/11 clearly suggests the states weigh their security and other public needs quite differently.

Similarly, we suspect there will not be a consensus in many of the subject areas covered in this conference, and there will be insufficient agreement to fashion model legislation for that mythical "any state."

We need also keep in mind that the federal government has been moving inexorably to preempt state decision making, and the availability of state records and information, quite possibly making more restrictive state law unnecessary. Indeed, the discussions at this conference may lead us to conclude that the best outcome in some subject areas is to suggest the states push back or hold back the federal efforts to turn what is and should remain public oversight information into new secrets.

The conference should consider not the drafting of a model law but rather the formulation of a set of broad principles designed to balance the competing values and interests, and a set of guidelines on the individual areas where our conversations suggest new or modified legislation might be needed.

This approach will be far more helpful, and almost certainly less polarizing.

1.2 Florida's Response to 9/11: The Impact on Open Government

by Barbara A. Petersen

It is time also to assert certain American fundamentals, foremost of which is the right to know what government is doing, and the corresponding ability to judge its performance

—Senator Daniel Patrick Moynihan[1]

Introduction: Florida's Open Government Laws

Florida has a very long, very rich tradition of open government—our first open meetings law was enacted in 1905[2] and the first public records law in 1909.[3] This exceptional tradition of public

1 U.S. Congress, Senate Comm'n on Protecting & Reducing Gov't Secrecy, S. Doc. 105-2, 103d Cong. (1997).

2 The 1905 open meetings law, ch. 5463, applied only to municipalities and was rendered virtually meaningless by a Florida Supreme Court decision nearly 50 years later. *See Turk v. Richard*, 47 So.2d 543 (Fla. 1950). The current law, § 286.011, F.S., was enacted in 1967. Fla. Ch. No 67-356.

3 Ch. 5492, 1909 Fla. Laws. Actually, the very first public records law, which provided that all records of the clerks of court "shall always be open to the public…for the purpose of inspection thereof, and of making extracts

access to government information culminated in the 1992 general election with passage of a new constitutional amendment guaranteeing a right of access to the records of all three branches of state government[4] and to "[a]ll meetings of any collegial public body of the executive branch of state government or of any…county municipality, school district, or special district at which official acts are to be taken or at which public business… is to be transacted or discussed."[5]

The breadth of Florida's open government laws is most apparent when the definition and interpretation of key words used in the statutes are considered. "Public records," for example, is broadly defined in statute as:

> …all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.[6]

A "meeting" for the purposes of the Sunshine Law is "*any* gathering, whether formal or casual, of two or more members of the same board or commission to discuss some matter on which *foreseeable action* will be taken by the public board or commission." [7]

The word "person"- those who have a right of access to the records and meetings of government- is defined in §1.01(3), of the Florida Statutes, to include not only individuals, but also "firms, associations, joint []ventures, partnerships, estates, trusts…corporations, and all other groups or combinations." Prior to 1975, the right of access to records was limited to state citizens, but today "the law provides any member of the public access to public records, whether he or she be the most outstanding civic citizen or the most heinous criminal,"[8] and a requestor's "motive in seeking access to public records is irrelevant."[9] Additionally, as a general rule, a person who makes a public records request or simply attends a public meeting cannot be required to provide identification. Thus,

---

therefrom" was enacted in 1892. Fla. Rev. S. 1390 – 1391.

4 Fla. Const. Art 1, § 24(a). Specifically, the amendment guarantees the "right to inspect and copy any public records made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf," including "the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, and districts; and each constitutional officer, board and commission, or entity created pursuant to law or th[e] Constitution." *Id*. Under the amendment, all exemptions in effect on the amendment's effective date – July 1, 1993 – remain in force until repealed, as are all rules of court adopted prior to the November 1992 election which control access to judicial records. The Florida Supreme Court adopted rules restricting access to certain judicial records, and the Legislature passed legislation regulating access to its records during Special Session 1993 B. *See In re Amendment to Rules of Judicial Admin.* – Public Access to Judicial Records, No. 80-419 (Fla. Oct. 29, 1992) (amending Fla. R. Jud. Admin. 2.051) (subsequently renumbered as Fla. R. Jud. Admin. 2.420); *and* Fla. SB 20-B (1993).

5 Fla. Const. Art 1, § 24(b).

6 Fla. Stat. § 119.011(11) (2007). The Florida Supreme Court has interpreted this definition to include *any* material made or received by an agency "which is intended to perpetuate, communicate or formalize knowledge" having to do with public business. *See Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc*., 379 So. 2d 633, 640 (Fla. 1980). This includes "all of the information" stored on a computer. *Seigle v. Barry*, 422 So. 2d 63, 65 (Fla. 4th DCA 1982), *pet. for review denied*, 431 So. 2d 988 (Fla. 1983).

7 Office of the Att'y General, Florida's Government-in-the-Sunshine and Public Records Law Manual 15 (Vol. 29 2007) [citing *Hough v. Stembridge,* 278 So. 2d 288 (Fla. 3d DCA 1973); *City of Miami Beach v. Berns,* 245 So. 2d 38 (Fla. 1971); *Bd. of Pub. Instruction of Broward County v. Doran,* 224 So. 2d 693 (Fla. 1969); and *Wolfson v. State,* 344 So. 2d 611 (Fla. 2d DCA 1977)] (emphasis in the original) [hereinafter 2007 Manual].

8 *Church of Scientology Flag Service Org., Inc. v. Wood,* No. 97-688CI-07 (Fla. 6th Cir. Ct. February 27, 1997).

9 *Timoney v. City of Miami Civilian Investigative Panel,* 917 So. 2d 885, 886 n.3 (Fla. 3d DCA 2005). *See also Curry v. State*, 811 So. 2d 736, 742 (Fla. 4th DCA 2002); *Staton v. McMillan,* 597 So. 2d 940, 941 (Fla. 1st DCA 1992), *review denied sub nom, Staton v. Austin*, 605 So. 2d 1266 (Fla. 1992); *Lorei v. Smith,* 464 So. 2d 1330, 1332 (Fla. 2d DCA 1985), *review denied,* 475 So. 2d 695 (Fla. 1985); and *News-Press Publishing Company, Inc. v Gadd*, 388 So. 2d 276, 278 (Fla. 2d DCA 1980).

anyone seeking access to Florida government - whether through a request for public records or attendance at a public meeting - can do so virtually anonymously.[10]

Furthermore, there is a presumption of openness under Florida law - that is, we *presume* that all agency records are subject to public disclosure and that any meeting of two or more members of the same collegial body at which public business is to be transacted or discussed will be open to the public. Because the Florida Constitution provides that only the Legislature can create exemptions to the public records and sunshine laws, there's no balancing of interests by a government agency or even the courts: a request for records can be denied or a meeting closed *only if* an agency has *specific* statutory authority.[11]

Finally, the Florida courts have consistently held that the right of access conferred by both the public records law and sunshine law - which were enacted for the public benefit - must be liberally construed in favor of open government and that any exception to that right of access must be narrowly construed and strictly applied. The right of access, then, "is virtually unfettered, save only the statutory exemptions designed to achieve a balance between an informed public and the ability of the government to maintain secrecy in the public interest."[12]

As the horror of 9/11 unfolded, public officials at all levels of government all over Florida scrambled to 'find' an exemption that would allow them to deny access to sensitive, security - related documents and to close meetings at which security measures were to be discussed and evaluated. The tension caused by the state's historical presumption of openness in a suddenly security - conscious government was palpable, and government officials and employees began to seriously question the efficacy of Florida's long tradition of public access.

SEPTEMBER 11, 2001: FLORIDA REACTS

The most tangible change in Tallahassee post - 9/11 was the obvious and dramatic increase in security. Having grown up in security-conscious Washington, DC, I was surprised by the lack of security in the capital city - only our public schools and the Supreme Court had metal detectors prior to the terrorist attacks of 9/11. This meant that the thousands of visitors to the state Capitol could freely enter and wander the halls pretty much at will, watched over only by a handful of armed and friendly capitol police officers. On a typical day it was not unusual to see the Governor or Attorney General walking to or from their capital offices or grabbing a cup of coffee in the basement cafeteria and it was entirely possible that you might meet the Senate President or House Speaker on one of the building's many elevators.[13]

---

10 *See* 2007 Manual, p. 42 (meetings) and pp. 112 – 113 (records).

11 *See* Fla. Const. Art 1, § 24(c). Under Art. I, s. 24(c), only the Florida legislature is allowed to create exemptions to the records and meetings requirements. Any exemption, however, must (1) pass by a two-thirds vote of each chamber, (2) contain a specific statement of public necessity, (3) be no broader than it's stated purpose, and (4) be in a single subject bill. *Id*. "Exemption" is defined as "a provision of *general law* which provides that a specific record or meeting, or portion thereof, is not subject to the access requirements of § 119.071(1), § 286.011, or § 24, Art. I of the State Constitution." Fla. Stat. § 119.011(8) (2007). Prior to enactment of the constitutional guarantee of access, the Florida Supreme Court had held that only the Legislature could create exemptions to the state's open government laws. *See Wait v. Florida Power and Light Company*, 372 So. 2d 420, 425 (Fla.1979).

12 *Times Publishing Company v. City of St. Petersburg*, 558 So. 2d 487, 492 (Fla. 2d DCA 1990). *See also Krischer v. D'Amato,* 674 So. 2d 909, 911 (Fla. 4th DCA 1996); *Seminole County v. Wood,* 512 So. 2d 1000, 1002 (Fla. 5th DCA 1987), *review denied,* 520 So. 2d 586 (Fla. 1988); *Tribune Company v. Public Records,* 493 So 2d 480, 483 (Fla. 2d DCA 1986), *review denied sub nom., Gillum v. Tribune Company,* 503 So. 2d 327 (Fla. 1987); and *Board of Public Instruction of Broward County v. Doran,* 224 So. 2d 693 (Fla. 1969).

13 Security in the state capitol had been relatively lax prior to the terrorist attacks of 9/11. In January 2000, two members of the Legislature's Black Caucus, Sen. Kendrick Meek (D-Miami) and Rep. Tony Hill (D-Jacksonville), took over the Governor's office suite for 20 hours, angry over the Governor's position on affirmative action and his refusal to meet with them to discuss the issue. The Governor eventually made several concessions, but only after

This relaxed atmosphere abruptly changed. Following the terrorist attacks on the World Trade Center and the Pentagon the physical security of public buildings became critically important - particularly in Tallahassee, home to President George W. Bush's brother, Jeb Bush, Florida's governor. All entrances to the Capitol but one were closed, forcing everyone to enter and exit through the same door. A metal detector was installed, manned by heavily armed law enforcement officers, and everyone – lobbyists, school children, legislative and administrative staff – was individually screened before allowed into the building. Many of the stairways were locked, and for the first time in at least recent memory, there was an armed guard protecting the entrance to the Governor's office.[14]

Within hours of the terrorist attacks the morning of 9/11 government officials around the state began to review security system plans, and called emergency meetings to discuss existing plans and the obvious need for heightened security measures. Governor Jeb Bush quickly declared a state of emergency, signing Executive Order 01 - 262 [15] that same day "giving the state almost unrestricted power for 60 days to 'regulate the movement of any and all persons to or from any location' as well as 'seize and utilize any and all real or personal property'."[16] Three days later, on September 14, the Governor directed the Florida Department of Law Enforcement (FDLE) and the Florida Division of Emergency Management (FDEM) "to immediately complete a comprehensive assessment of Florida's capability to prevent, mitigate, and respond to a terrorist attack," requesting a full report within two weeks.[17]

The report contained a series of rather obvious and practical recommendations that included implementation of regional anti-terrorism task forces, a significant increase in law enforcement training and the purchase of necessary equipment, the collection and sharing of information, and coordination of communication between state and federal agencies.[18] Other recommendations which became a lightening rod for criticism by civil libertarians and a number of conservative legislators included a proposal that would allow law enforcement "to detain for a reasonable period of time those individuals suspected of terrorist activities and involvement" and expansion of wiretap and surveillance capabilities.[19] The report also made a

about 100 people supporting the two legislators waged a day-long sit-in outside the Governor's office in the Capitol. *See* Steve Bousquet & Lesley Clark, *Sit-In Ends*, The Miami Herald, Jan. 20, 2000.

14 *See* Editorial, The Daytona Beach News-Journal, Oct. 22, 2001. The new capitol security was truly tested during the Terri Schiavo controversy, when a small number of state Senators, opposed to legislation that would have allowed Ms. Schiavo's parents to reinsert her feeding tube requested armed escort from their legislative offices to the Senate Chamber after threatening "wanted" posters with the Senators' pictures were hung in the state Capitol. *See* Mark Caputo, *Security Tightens Around Capitol*, The Miami Herald, Mar. 23, 2005.

15 Fla. Exec. Order 01-262, Emergency Management, Sept. 11, 2001.

16 Diane Roberts*, Op-Ed: Sunshine Laws Remain Intact – So Far,* St. Petersburg Times, Nov. 4, 2001 [hereinafter Roberts Nov. 4 Op-Ed]. The order was set to expire in November 2001, but was subsequently expanded until January 2002. *See* Lesley Clark, *State Makes Security a Priority Despite Cost,* The Miami Herald, Dec. 16, 2001.

17 *See* Florida Department of Law Enforcement and the State Division of Emergency Management, *Assessing Florida's Anti-Terrorism Capabilities*, p. 1 (Sep. 2001) [hereinafter FDLE Report]. *See also* Fla. Exec. Order 01-300, Oct. 11, 2001.

18 FDLE Report, p. 3 (implementation of regional anti-terrorism task forces; appropriate training for all response personnel); p. 4 (identify and obtain appropriate equipment); p. 4 (enhance retrieving, storing and sharing vital intelligence and investigative information); and p. 5 (coordinate communication between responding agencies).

19 *Id*. at pp. 5–6. Larry Spalding of the American Civil Liberties Union expressed grave concerns not only about the expansion of police powers and the creation of secret files, but also the loss of privacy as government officials proposed "to lengthen the period suspected terrorists could be detained, conduct background checks on people who work in airports and seaports, and provide immunity from lawsuits for those who inform police about suspicious activity or people." Laura Zuckerman, *Civil Liberties Groups Fear Loss of Privacy*, The Daytona Beach News-Journal, Oct. 3, 2001. Sen. Alex Villalobos, R-Miami, in

series of recommendations regarding the public's right of access to government records.[20] These recommendations would prove extremely controversial in the coming months.

In the meantime, concern among public officials in Florida rose to near panic as news reports about the terrorists' activities in the weeks and months prior to 9/11 began to emerge. Fifteen of the nineteen terrorists involved in the attacks lived or trained in Florida. Thirteen had valid Florida drivers' licenses. The state began to view itself "as a hotbed of terrorist training."[21] In response, the Florida Department of Highway Safety and Motor Vehicles shut down access to motor vehicle and driver history records, asking that "all agents of [the] department…refrain from processing public [record] requests" for such records "until further notice."[22] Attempting to justify the Department's action, a spokesman for the department said the records had to be withheld in order to avoid compromising ongoing investigations and noted that law enforcement agencies had asked for a narrower embargo, that only those records of "certain nationalities who obtained their licenses during a certain period of time" be withheld.[23] There was also the added concern that the media was one step ahead of law enforcement, and Florida's top law enforcement officer "complained that '[s]ometimes…the media get to a suspect or a material witness before the police do, alerting others who may be involved in terrorist activity and allowing them to escape'."[24]

The Florida Legislature acted quickly as well. Within just a few days of the terrorist attacks it created special committees - the Select Committee on Public Security and Crisis Management in the Senate, chaired by Sen. Ginny Brown-Waite, R-FL/Brooksville, and the House Select Committee on Security, chaired by Rep. Dudley Goodlette, R-FL/Naples, to perform the dual task of studying state security and coordinating Florida's response to the national emergency. [25] According to a press release from House Speaker Tom Feeney, R-FL/Oviedo, "[t]he tragedies of Sept. 11 have prompted a nationwide effort to improve security measures, and it is important that the [Florida] House

response to the proposal to hold suspected terrorists while their arrests remained secret, expressed the concern "that we have a balancing question here about the right of the public to be protected but also the right of the accused to know what they are accused of." In direct contrast, Sen. Ron Silver, D-North Miami Beach, had this response to the same proposal: "I know the constitution is out there, and I know we want to abide by it, but there's some wiggle room there." *See* Nancy Cook Lauer, *Senate Panel Scrutinizes State Security*, Tallahassee Democrat, Oct. 11, 2001.

20 *See* FDLE Report at pp. 5 – 6.

21 Joe Follick, *State Security Panels Born in Legislature,* Tampa Tribune, Sept., 25, 2001 [hereinafter Follick Sept. 25 Article]. *See also* Mark Silva and Maya Bell, *Floridians are Living in New State of Alert,* The Orlando Sentinel, Oct. 11, 2001.

22 Memo from Sandra C. Lambert, Director, Division of Driver Licenses, and Carl A. Ford, Director, Division of Motor Vehicles, Sept. 18, 2001. Similarly, the Florida Department of Agriculture refused to release a list of 150 "aerial applicators" pursuant to a public records request from *The Palm Beach Post*, giving the list instead to the Florida Department of Law Enforcement, which also denied the *Post's* request. *See* Jim Ash, *Security Concerns Threaten State's Open Records, Meetings Law,* The Palm Beach Post, Sept. 26, 2001 [hereinafter Ash Sept. 26 Article].

23 Steve Bousquet, *Drivers Records Put on Hold*, St. Petersburg Times, Sept. 20, 2001 (quoting Bob Sanchez, spokesman for the Department of Highway Safety and Motor Vehicles).

24 Roberts Nov. 4 Op-Ed (quoting Tim Moore, Commissioner of the Florida Department of Law Enforcement). Criticism of the Department's action was swift and furious. *See, e.g.,* Steve Bousquet, *Drivers Records Put on Hold*, St. Petersburg Times, Sept. 20, 2001; Editorial, *No Time to Seal Records*, The Orlando Sentinel, Sept. 24, 2001; and Editorial, *Public Records Are Public, Period,* St. Petersburg Times, Sept. 26, 2001. Under Florida law, a government agency can deny a request for public records only if there is a specific statutory exemption applicable to the records requested and at the time, motor vehicle and driver history records were subject to public disclosure. Thus, the Department's action was a direct and clear violation of Florida's constitution and the records withheld by the Department were clearly subject to public disclosure under Florida law. *See* Fla. Const. Art. I, § 24. *See also, Memorial Hospital-West Volusia v. News-Journal Corporation,* 729 So. 2d 373 (Fla. 1999).

25 Follick Sep. 25 Article.

of Representatives is equipped with the most current knowledge and technological information on anti-terrorism available."[26]

After anthrax was discovered at the American Media, Inc. headquarters in Boca Raton, FL in late September,[27] Florida's economy, deeply dependent on tourism, experienced an immediate downturn. Faced with a $1.3 billion budget shortfall as a result of the drop in tourism, Governor Bush called a special session of the Legislature, set to run from October 22 through November 1, 2001, "for the sole and exclusive purpose of considering the reductions to this fiscal year's appropriations from the general revenues of the state that are needed to deal with the anticipated decline in revenue in the aftermath of [the] acts of terror."[28]

But as "[t]he terrorist assaults of Sept. 11 and unexplained anthrax attacks…created a sense of emergency about protecting everything from seaports to water utilities," and Florida's chief law enforcement officer Tim Moore, pushed hard for "new exemptions to Florida's public records law…needed to keep sensitive information from the hands of terrorists,"[29] the Governor expanded the legislative call to include consideration of "legislation necessary for security and economic stimuli."[30]

Ultimately, it took two special legislative sessions to achieve the Governor's goal, as the first, Special Session 2001 B, ended in partisan bickering and legislative "hissy fits," and without a meaningful fiscal fix.[31] And although Governor Bush called the first special session "a qualified success,"[32] he nevertheless called the Legislature back to Tallahassee for a second attempt at dealing with "security and economic stimuli matters important to Florida."[33]

26 Ash Sept. 26 Article. In creating the new security committee, House Speaker Feeney raised the possibility of closed-door committee meetings. *See* Id., *and* Letter from Tom Feeney, Florida House Speaker, to the First Amendment Foundation (Sept. 25, 2001) [hereinafter Feeney Letter]. (Letter on file with the First Amendment Foundation, Tallahassee, FL.) The Speaker eventually backed away from the idea and ultimately urged moderation as the Senate considered sweeping changes to Florida's public records law and amended its rules to allow closed-door meetings, as did Governor Jeb Bush. *See, e.g.,* Lesley Clark, *Senators Approve Secret Committee Meetings,* The Miami Herald, Oct. 26, 2001; Mark Silva, *Vote Oks Meeting in Secret on Terror, Sun-Sentinel*, Oct. 26. 2001; and Editorial, *Feeney's Stand*, The Orlando Sentinel, Dec. 9, 2001 [hereinafter Orlando Sentinel Dec. 9 Editorial]. *See also* pp. 24 – 27, supra.

27 Barbara Perez, *The Latest,* The Orlando Sentinel, Oct. 17, 2001. American Media is publisher of The Sun and other supermarket tabloids. Ultimately, seven of company's employees became ill after exposure to the anthrax bacteria, and one, Robert Stevens, died on October 5, 2001. *Id.*

28 Executive Office of the Governor, Proclamation to the Honorable Members of he Florida Senate and House of Representatives, Oct. 10, 2001. After meeting with state tourism officials, Gov. Bush also hit the publicity trail, exhorting visitors to return to Florida. *See* Editorial, *Mr. Tourism, Jeb Bush*, The Orlando Sentinel, Oct. 3, 2001, and Roberts Nov. 4 Op-ed.

29 Mark Silva, *Sunshine Law Faces Shadow*, The Orlando Sentinel, Oct. 29, 2001 (quoting Tim Moore, Commissioner of the Florida Department of Law Enforcement). A number of law enforcement officers "pledged 'to work like the dickens' to add new exemptions" to the public records law "and at least one legislator suggested 'a complete suspension of the public records act during an emergency.'" Lucy Morgan and Steve Bousquet, *Lawmakers Might Place Limits on Public Records,* St. Petersburg Times, Oct. 17, 2001.

30 Executive Office of the Governor, Proclamation to the Honorable Members of the Florida Senate and House of Representatives, Oct. 25, 2001.

31 *See* Roberts Nov. 4 Op-Ed. *See also* Editorial, *Budget Time, Again,* St. Petersburg Times, Nov. 27, 2001. The two post-911 special sessions followed the 2001 regular session and were thus given letters to note the order. Special Session 2001 A was an organizational session that preceded the regular session.

32 Jim Ash, *Legislature's Special Session Yields Few Anti-Terrorism Laws*, The Palm Beach Post, Nov. 1, 2001 [hereinafter Ash Nov. 1 Article].

33 Executive Office of the Governor, Proclamation to the Honorable Members of the Florida Senate and the House of Representatives, Nov. 6, 2001. Special Session 2001 C was set to run from November 27 through December 6, 2001.

SPECIAL SESSION 2001 B

As the Legislature prepared to meet in its first special session after the terrorist attacks of 9/11, State Senator Rod Smith, D-FL/Gainesville, "expressed concern about the need" for amendments to Florida's public records law "in light of recent terrorist acts" and asked Attorney General Bob Butterworth to "examine existing statutory exemptions relating to security and criminal investigations conducted by law enforcement agencies."[34] Specifically, Senator Smith sought an opinion on whether "current statutes provide an exemption from disclosure for materials such as security systems plans or security needs assessments that are on file with a public agency."[35]

At issue was the scope and breadth of § 281.301, F.S., which provided an exemption for information relating to security systems plans for "property owned by or leased to the state or any of its political subdivisions," as well as all meetings "that would reveal such systems or information." The exemption, first enacted in 1987, was expanded a few years later to also include "information relating to the security systems for a privately owned or leased property, when such information is in the possession of any agency."[36] "Information relating to the security systems" held by an agency specifically included

> all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to or revealing such systems or information.[37]

In noting that earlier opinions from the Attorney General found that the scope of the security systems exemption also included "blueprints[] on file from private entities for crime prevention purposes" and security needs assessments held by a government agency, Attorney General Butterworth opined that "[t]he comprehensive scope of the exemption makes it *unnecessary…to create additional exemptions* that would target this type of information."[38]

Senator Smith was also concerned with disclosure of active criminal investigative or intelligence information, and asked the Attorney General whether a criminal justice agency would be required to provide access to public records gathered as part of an active investigation.[39] Referencing a long-established public record exemption for active criminal investigative and intelligence information,[40] Attorney General Butterworth noted, "[i]t is well established in Florida that the exemption for active criminal intelligence and investigative information does not exempt other public records from disclosure simply because they are transferred to a law enforcement agency."[41] However, the opinion continued,

> …the Public Records Act cannot be used to elicit exempt or confidential material. As one appellate court observed: The Public Records Act "may not be used in such a way to obtain information that the legislature has declared must be exempt from disclosure." Thus, the exemption for active criminal investigative information may not be subverted by making a public records request for all public records gathered by a law enforcement agency in the course of its investigation; to permit such requests would negate the purpose of the exemption.[42]

34 Op. Att'y Gen. Fla. 01-75 (2001) at p. 1 [hereinafter AGO 01-75].
35 *Id*.
36 *See* Staff of Fla. H.R. Committee on Governmental Operations, Final Staff Analysis & Economic Impact Statement on HB 2513 (1990) at 9.
37 Fla. Stat. § 281.301, F.S. (2001)
38 AGO 01-75 at p. 3. (emphasis added)
39 *Id*. at p. 1.
40 *See* § 119.07(3)(b) (2001). Recodified as § 119.071(2)(c)1 (2007).
41 AGO 01-75 at p. 4 (citation omitted).
42 *Id*. citing *City of St. Petersburg v. Romine ex rel.*

The Attorney General concluded that a "law enforcement agency would not be required to respond to a public records request which would divulge the existence of an ongoing active criminal investigation or active criminal intelligence operation."[43] Yet despite the Attorney General's opinion that existing law was sufficient to protect security-related information and active criminal investigative information and that additional exemptions were unnecessary, during its first special session, Special Session 2001-B, the Florida legislature, at the urging of the state's chief law enforcement officer, filed and considered a plethora of new exemptions to the public records law.

And although all the proposed exemptions were filed in response to new security concerns raised by the terrorist attacks of 9/11-including legislation that would close access to the billing records for a law enforcement officer's cellular telephone and a bill that would exempt the FAA (Federal Aviation Administration) aircraft registration numbers of aerial applicators-not one of the proposed exemptions passed, due in some measure to constitutional and public policy objections raised by the open government advocates, civil libertarians, and the media, but also to the extreme lack of cooperation between Florida's legislative leaders.[44] Put simply, the House Speaker and the Senate President did not get along.

However, many of the exemptions considered were re-filed in the 2002 regular session and other subsequent sessions, and the Senate amended its rules to allow it to meet in secret and, in direct contravention to the state constitution, to deny access of records relating to the secret meetings.

Special Session 2001 B: Legislative Proposals

CS/SB 58-B and HB 121-B, Hospital Emergency Management Plans

Originally filed as a shell bill,[45] SB 58-B was amended and unanimously approved by the Senate Committee on Governmental Oversight and Productivity.

Dillinger, 719 So. 2d 19, 21 (Fla. 2d DCA 1998).

43 *Id.*

44 *See, e.g.,* Roberts Nov. 4 Op-Ed. *See also* Editorial, *Special Session Caution*, St. Petersburg Times, Oct. 23, 2001; Mary Ellen Klaus, *Bills would Let Police Skirt Sunshine Law*, Palm Beach Post, Oct. 23, 2001; Wire Services, *Key Senate Panel Goes Down Security Proposals*, The Daytona Beach News-Journal, Oct. 23, 2001; Mark Silva, *Florida Politics: Rash Rush to Secrecy*, The Orlando Sentinel, Oct. 28, 2001; and Liz Balmaseda, *Secret Meetings? Not a Good Move,* The Miami Herald, Oct. 29, 2001. Although Special Session 2001B ended in near complete failure, the Legislature did manage to pass a number of bills designed to foster patriotism – a bill requiring school children to recite the Pledge of Allegiance was approved, as was legislation allowing home owners to fly the American flag regardless of homeowner association rules. *See* Editorial, *Cheap Political Trick,* The Orlando Sentinel, Oct. 24, 2001; and Pamela Hasterok, *Vantage Point: A Red, White and Blue Cover-Up,* The Daytona Beach News-Journal, Oct. 25, 2001. In casting the sole vote against the bill requiring recitation of the Pledge of Allegiance, which is unconstitutional, Rep. Chris Smith, D-Fort Lauderdale, expressed his frustration: "In their extreme zealousness to show their extreme patriotism, they've got us violating the Constitution. If they suggested everyone has to tattoo a flag on their butt, everyone would have voted for that." Editorial, *Legislative Follies,* The Miami Herald, Oct. 25, 2001. In addition, the Legislature approved two new specialty license plates – United We Stand and American Red Cross – with proceeds to be used "to support airport security, poison control centers, and a federal reward program for terrorist snitches." *See* Ash Nov. 1 Article.

45 Interestingly, all of the open government bills filed in the Senate during Special Session 2001 B were "shell" bills, and all had identical language: "It is the intent of the Legislature to create an exemption from public-records requirements in response to acts of terrorism." Shell bills have become ubiquitous in the Florida Senate, due in large part to Senate rules, strict filing deadlines, and the single subject requirement under Art. I, sec. 24 of the Florida Constitution for any bill creating a exemption to either the public records law or sunshine law. A shell bill is, in effect, a place-holder, filed by the sponsor in a timely fashion and later amended by a strike-all amendment adding substance to the legislation. According to the First Amendment Foundation, which tracks all open government legislation each session, there were 14 shell bills filed in the 2007 session, 4 of which were later amended to create new open government exemptions. *See* First Amendment Foundation, Final Report 2007 Legislative Session, May 5, 2007 (Report on file with the First Amendment Foundation, Tallahassee, FL).

As amended, CS/SB 58-B would create a public records exemption for portions of a comprehensive emergency-management plan which address the response of a public or private hospital to an act of terrorism, including those portions addressing security systems or plans; vulnerability analyses; emergency evacuation transportation; sheltering arrangements; post-disaster activities and transportation; supplies, including drug caches; staffing; emergency equipment; and individual identification of residents, transfer of records, and methods of responding to family inquiries. The bill also contained a provision that would exempt portions of public meetings relating directly to or revealing information regarding such plans. Finally, although the bill stipulated that the certification of the sufficiency of a hospital's emergency response plan by the Governor would be a public record, the legislation did not require such certification.

According to the bill's constitutionally - required statement of public necessity, the Legislature determined that a hospital's emergency response plan "could be used to hamper or disable the response of a hospital to a terrorist attack," in which case "an increase in the number of Floridians subject to fatal injury would occur." The Legislature further found that

> [w]hile some skill would be required to use knowledge of plan components to disable a hospital response to an act of terrorism, there is ample existing evidence of the capabilities of terrorists to plot, plan, and coordinate complicated acts of terror. The hijacking and crashing of planes, the destruction of the World Trade Center, the attack on the Pentagon on September 1, 2001, as well as the continued and purposeful spread of anthrax in Washington, D.C., other states, and communities within this state, which has resulted in the death of at least one Floridian, provide evidence of such skill. [46]

HB 121-B, amended by the House Select Committee on Security to conform to its Senate companion, was unanimously approved by the committee, and passed out of the House the following day by a vote of 118/0, but died in the Senate without a hearing. The CS/SB 58-B died on the Senate Calendar. However, similar legislation was approved during the following session, Special Session 2001 C.[47]

CS/SB 60-B and HB 123-B, Pharmaceutical Materials and Depositories

Also filed originally as a shell bill, SB 60-B was amended and unanimously approved by the Senate Committee on Governmental Oversight and Productivity.

As amended, CS/SB 60-B would create a public record exemption for the type or amount of pharmaceutical materials as well as the location of any pharmaceutical depository maintained in order to respond to an act of biochemical terrorism. Again, although the legislation stipulated that a certification of the sufficiency or amount of the pharmaceutical or the security of the depository would be public record, there was no requirement that such a certification be made nor any information on what agency might be responsible for the certification.

In justifying the exemption, the Legislature once again made reference to the possible use of such information "in planning acts of terrorism,"

46 Fla. CS/SB 58-B (2001) at p. 3 – 4. Similar and sometimes near-identical language can be found in many of the security-related exemptions filed during Special Session 2001 B and subsequent sessions. *See, e.g.*, Fla. CS/SB 60-B (2001) at p. 2 (proposed exemption for pharmaceutical cache information); Fla. HB 41-C (2001) at p. 3 (proposed expansion of security systems plan exemption); Fla. SB 970 (2002) at p. 3 (proposed aerial applicators exemption); and Fla. CS/CS/SB 1362 (2003) (proposed exemption for building plans, blueprints, etc., of certain privately owned facilities).

47 *See* Fla. CS/SB 18-C, *supra*.

stating that

> [i]f terrorists were able to determine what types of pharmaceuticals are stored or maintained for response to terrorism, or the amount of pharmaceuticals stored, they could use this information to craft a terrorist act to which the state may not be as well prepared to respond. This information could be used to increase the number of people injured or killed in a terrorist act.[48]

HB 123-B was, again, amended to conform to its Senate companion, and approved unanimously by the House Select Committee on Security. The bill passed out of the House with a vote of 118/1 and died in Senate Messages. The CS/SB 60-B died on the Senate Calendar, but similar legislation was approved during Special Session 2001 C.[49]

CS/SB 62-B and HB 125-B, Security Systems Plans

Although the Attorney General had opined that the "comprehensive scope" of the exemption for security systems plans under § 281.301, F.S., made any amendment unnecessary,[50] legislation was filed during Special Session 2001 B that would slightly expand the exemption. Under the law in place at the time, all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations revealing security systems were exempt, as was any meeting relating directly to such systems plans. The CS/SB 62-B would have expanded the exemption to include threat assessments, threat response plans, emergency evacuation plans, sheltering arrangements, and manuals for security personnel, emergency equipment, or for security training with its scope of protection.[51]

Like the other proposed exemptions filed in the Senate, SB 62-B was originally filed as a shell bill and later amended and unanimously approved by the Senate Committee on Governmental Oversight and Productivity; the public necessity language in Section 2 of the bill was virtually identical to that in CS/SB 58-B.[52]

A strike-all amendment to HB 125-B, approved unanimously by the House Select Committee on Security, conformed the House bill to its Senate companion with one significant difference: HB 125-B moved the security systems exemption into chapter 119, F.S., the public records law, which would make it much easier to find.[53] Although both the Senate and House bills subsequently died in the Senate, similar legislation was reintroduced and passed during Special Session 2001-C.[54]

CS/SB 64-B and HB127-B, Law Enforcement Officers/Cellular Telephone Numbers

A shell bill, SB 64-B was amended by the Senate Committee on Governmental Oversight and Productivity to create a public record exemption for the cellular telephone number of a law enforcement officer or former officer used in the course of his or her employment. Somewhat surprisingly, the sponsors of the legislation and its companion bill, HB 127-B, couched the necessity for the exemption under the rubric of security, claiming that access to a law enforcement officer's cellular

48 Fla. CS/SB 60-B (2001) at p. 2.
49 *See* Fla. CS/SB 20-C, *supra*.
50 AGO 01-75 at p. 3.
51 Fla. CS/SB 62-B.
52 *See* Fla. CS/SB 62-B at p. 3.
53 There are well over 1,000 exemptions to Florida's public records law and sunshine law, and only a handful of those exemptions are actually in the substantive chapters. The rest, the vast majority, are scattered throughout the statutes and can be difficult to locate (for example, § 281.301, F.S., was codified under title XIX, Safety and Security Services) , and the burden is on the custodial agency denying a public record request to provide the exact statutory citation authorizing the denial. *See* § 119.07(1)(c) and (d), F.S. (2007). Transferring the exemption to ch. 119, the Public Records Law, made practical sense.
54 *See* Fla. CS/SB 16-C, *supra*. The CS/SB 62-B died on the Senate Calendar; HB 125-B passed the House by a vote 116/1 and died in Senate Messages.

telephone number could compromise an on-going criminal investigation.[55] The House version was broader than its Senate companion, including cellular billing records within the scope of the exemption.

Although both bills were approved unanimously by their respective committees of reference, each died on the calendar. Similar legislation was filed in various subsequent sessions and failed to pass.[56]

CS/SB 66-B and HB 129-B, Law Enforcement Officers/Electronic Pager Numbers

Nearly identical to the proposed exemption for a law enforcement officer's cellular telephone number and containing the same questionable public necessity language, CS/SB 66-B, as amended, would create a public record exemption for the electronic pager number of a law enforcement officer or former officer used in the course of his or her employment. Its companion, HB 129-B, would also exempt the related billing records. Again, each bill was unanimously approved in committee, but died on their respective calendars without consideration

CS/SB 68-B and HB 131-B, Automatic Delay/ Public Record Requests

As controversial as it was unconstitutional,[57] CS/68-B, as amended and approved by the Senate Governmental Oversight and Productivity Committee, would create a mechanism by which the Florida Department of Law Enforcement (FDLE) automatically delay for at least a week (with the exception of arrest records or records of first appearance) normally open to inspection and copying for the purpose of preventing or investigating acts of terrorism. The legislation required an agency to delay the inspection or copying of a public record for up to seven days if the FDLE executive director requested the delay and certified in writing (1) the specific record for which access was to be delayed; that (2) the record was necessary for investigation of a threat of a terrorist act; (3) the record was part of an active criminal investigation or was active criminal intelligence information; (4) access would jeopardize the ability of law enforcement to prevent or reduce the threat of an act of terrorism; and (5) the specific time period during which access is to be delayed.

In addition, after an in-camera review of the requested records and upon a showing by substantial competent evidence by the FDLE that (1) a viable threat of a terrorist act exists; (2) the public record at issue is active criminal intelligence or investigative information related to the threat; and (3) access would jeopardize the ability of law enforcement to prevent or reduce the threat, a court could extend the delay for an additional fourteen days, meaning, of course, that a request for public records could be delayed by the FDLE for as long as three weeks.[58]

The House companion, HB 131-B, was similar except that it would allow FDLE to automatically close records for an initial period of only 48 hours, at which point FDLE would be required to seek a court order allowing an additional 14-day delay.[59]

The constitutionally-required statement of

55 *See* Fla. CS/SB 64-B at p. 2; *see also* Fla. HB 127-B at p. 2.

56 *See, e.g.,* Fla. HB 737 (2002) (cellular telephone numbers & billing records); HB 739 (2002) (digital pager numbers & billings records); HB 123 and SB 1666 (2003) (cellular telephone & digital pager numbers & related billing records); *and* SB 2370 (2004) (cellular telephone & digital pager numbers & related billing records).

57 *See, e.g.,* Wire Services, *Key Senate Panel Goes Down Security Proposals*, The Daytona Beach News-Journal, Oct. 23, 2001; Laura Zuckerman, *Focus of Bills: Tighten Security*, The Daytona Beach News-Journal, Oct. 30, 2001 [hereinafter Zuckerman Oct. 30 Article]; Earl Maucker, *Column: Security, Openness Require Delicate Balance*, South Florida Sun-Sentinel, Nov. 25, 2001; and David Twiddy, *Public Records Bill Looks Dead*, Tallahassee Democrat, Nov. 29, 2001 [hereinafter Twiddy Nov. 29 Article].

58 *See* Fla. CS/SB 68-B (2001).

59 *See* Fla. CS/HB 131-B (2001).

public necessity was identical in both bills, and bears recitation in its entirety:

> The Legislature finds that delay in the ability to inspect or copy a public record provided by this act is a public necessity because of the great potential for harm to the public which exists in this era as a result of terrorism. An act of terrorism may come in an entirely unusual form and terrorists may use unexpected and unconventional methods. The potential for acts of terror performed in unthinkable ways was made amply evident by the events of September 11, 2001. Individuals who resided, worked, and attended flying school in this state commandeered planes, murdered those on board who attempted to stop them, and then intentionally crashed those planes into the Pentagon and the World Trade Center, completely destroying the two main towers and surrounding structures. These acts of terror resulted in the deaths of approximately 6,000 persons. In addition, since that date, spores of anthrax have been purposefully distributed by persons yet unknown in Washington, D.C., other states, and communities within this state, in order to spread disease and cause death. As of this date, at least one Floridian has died because of anthrax, and other Floridians are being treated for the illness. Prior to these events, these methods of spreading destruction, death, and mayhem were unthinkable. The Legislature notes that, given the willingness of terrorists to die in the performance of acts of terror, it many not be able to foresee the manner or method in which an act of terrorism might be performed or the public information that could be used to facilitate or plan it. The Legislature, therefore, cannot foresee every public record that it must make confidential pursuant to its authority under s. 24(a), Art. I, of the State Constitution, in order to stop acts of terror. Given the capabilities of modern-day terrorists, as evidenced by the acts of September 11, 2001, and the potential that even more serious acts of terrorism could be perpetrated, the Legislature explicitly finds that state law enforcement investigations of acts of terrorism are of the highest priority and that there may be instances, which are yet unknown and unidentifiable, when the ability to inspect or copy a public record could jeopardize such an investigation by making the subjects of such investigations aware that an investigation is active. If it is discovered that an act of terrorism is being investigated, the perpetrators may speed up the timetable for the performance of the activity, as well as flee, destroy evidence, or evade prosecution. As the danger posed to the public is so extreme, and as it may become imperative at times to temporarily delay access to specified public records in order to prevent the imminent commission of an act of terrorism, the Legislature finds that the procedures provided in this act to temporarily delay inspection or copying of a specific public records that are part of an investigation into a potential act of terrorism are reasonable and in the best interests of the safety of the public. As a result, the Legislature finds that there is a substantial justification and public necessity for permitting the head of a law enforcement agency to request delay in the inspection or copying of public records under the limited circumstances and procedures set forth in this act.[60]

The legislation was in direct conflict with the constitutional standard for creation of new exemptions under Article I, section 24(c), of the Florida Constitution. Under the constitutional standard, any exemption to the right of access to government records guaranteed under section 24(a) must

60 Fla. CS/SB 68-B (2001) at pp. 3 – 5; and Fla. HB 131-B at pp. 3 – 5.

be narrowly-tailored. And in allowing the FDLE to determine which records would be exempt from public disclosure-even for a short period of time-the legislation violated the constitutional provision stipulating that only the Legislature could create exceptions to the right of access.[61] In addition, the public necessity statement appears to ignore the Attorney General's opinion-requested by Senator Rod Smith, sponsor of CS/SB 68-B-in which the General opined that "a law enforcement agency would *not* be required to respond to a public records request which would divulge the existence of an ongoing active criminal investigation."[62]

The CS/SB 68-B was unanimously approved by the Senate Committee on Governmental Oversight and Productivity, but died on the Senate Calendar. After members of the House expressed concerns about the bill's impact on Florida's open government laws,[63] HB 131-B was temporarily postponed and never made it out of committee. According to the bill's sponsor, Representative Dan Gelber, D-FL/Miami Beach, there were simply too many concerns about the bill's potential to violate the state constitution. "It's very difficult to reconcile (HB 131-B) with the Florida Constitution."[64] Identical legislation was filed again in Special Session 2001 C, but failed again to pass.[65]

CS/SB 70-B and HB 133-B, Law Enforcement Transmittal Letter

The least controversial open government legislation filed during the special session, CS/SB 70-B, and its companion, HB 133-B, was an attempt to clarify the law.[66] As amended, the legislation would create a public records exemption for a custodial agency's response to a request for public records from a law enforcement agency for records pursuant to an active criminal investigation. The bill required the law enforcement agency to notify the custodial agency when the investigation was complete or no longer active, at which point the transmittal letters would be subject to public disclosure.

Both bills were approved unanimously by their committees of reference and CS/SB 70-B died on the Senate Calendar. The HB 133-B, which passed the House by a vote of 116/2, died in Senate Messages. Near identical legislation was filed and passed in Special Session 2001 C.[67]

CS/SB 72-B and CS/HB 115-B, Department of Agriculture/Proof of Identification

Originally filed as a shell bill and amended by the Senate Agriculture Committee, CS/SB 72-B contained various provisions that would codify an emergency rule adopted by the Department of Agriculture on September 27, 2001. The rule required aerial applicators-crop dusters-"to provide information demonstrating proper pesticide registration, Federal Aviation Administration (FAA) licensure and aircraft registration. The emergency rules also require[d] the submission of daily flight plan information to authenticate operations if needed by law enforcement."[68]

During the Senate bill's only committee hearing, a handwritten amendment sponsored by Sen. Kendrick Meek, D-FL/Miami, to require a written request and two forms of personal identification from any person requesting certain, specified records from the Department of Agriculture, was adopted. In addition, the Meek amendment authorized the Department to give the written requests to any law enforcement agency for purposes of identify verification.[69]

61 *See* Fla. Const. Art 1, § 24(c).
62 AGO 01-75 at p. 4.
63 *See* Zuckerman Oct. 30 Article.
64 Twiddy Nov. 29 Article. Although Rep. Gelber was specifically referring to HB 53-C, filed during Special Session 2001-C, the bills were identical and thus gave rise to the same constitutional issues.
65 *See* Fla. SB 28-C; and HB 53-C, *supra*.
66 *See* AGO-01-75.
67 *See* Fla. SB 22-C, *supra*.
68 Staff of Fla. Sen. Agriculture Committee Staff Analysis of SB 72-B (2001) at pp. 1 – 2.
69 *See* Fla. CS/SB 72-B, s. 6 at p. 4. (The Meek

Interestingly, and perhaps a bit surprisingly, the House companion, HB 115-B, which was identical to CS/SB 72-B, was amended in the House Select Committee on Security to *remove* language identical to the Meek amendment. The amendment to HB 115-B removing the offensive language was offered by the bill's sponsor, Representative Dudley Goodlette, R-FL/Naples. The enrolled version of the House bill contained only those provisions that would regulate aerial applicators and the use of pesticides.[70]

After unanimous approval by the Senate Agriculture Committee, CS/SB 72-B was placed on the Senate Calendar where it died. The CS/HB 147-B passed the House unanimously and died in Senate Messages.

HB 147-B, Aerial Applicators

Filed in response to the fear that terrorists might use aerial applicator aircraft for application of biological or chemical agents,[71] HB 147-B would create a public record exemption for the names, addresses, and restricted-use license numbers of any person engaged in aerial application of pesticides, fertilizers, or seed, as well as the FAA aircraft registration number of any aircraft used for aerial application. The legislation seemed rather impractical, frankly. Most, if not all of the information at issue is available from a wide variety of other public and private sources. For example, crop dusters routinely advertise their services in local telephone books providing, obviously, their names and addresses. The FAA regulations require registration numbers to be painted on the fuselage of all registered aircraft, meaning such numbers are clearly visible from any highway near an airport or runway, and restricted-use license numbers and the aircraft registration numbers of all pilots and registered aircraft are available on the FAA's website.[72] Although introduced, HB 147-B did not receive a committee reference, and died, reference deferred. There was no Senate companion.

Senate Rule Change

"[T]he biggest step … to block the public's right to know in the wake of the Sept. 11 terrorist attacks"[73] was a change to Senate rules, allowing the Senate President to close meetings to discuss "measures to prevent possible acts of espionage, sabotage, attack and other acts of terrorism." As originally drafted, the rule amendment also closed all records "made or received during or in preparation for a closed meeting," including all votes taken at the secret meeting.[74]

Article III, section 4(e) of the Florida Constitution stipulates that all meetings of more than two legislators at which pending or proposed legislation is to be discussed must be reasonably opened

Amendment is on file with the First Amendment Foundation, Tallahassee, FL.) Specifically, the provision applied to requests for records or information under chapters 487 (Florida Pesticide Law and Agricultural Worker Safety Act), 570 (Department of Agricultural & Consumer Safety), 576 (Agricultural Fertilizers), and 578 (Florida Seed Law), of the Florida Statutes. As discussed previously, to require a written request and proof of identification as a condition to obtaining copies of public records is contrary to long-settled public policy in Florida, and to allow verification of the requestor's identity by a law enforcement agency is particularly offensive to the state's rich tradition of openness. *See* Introduction, pp. 1 – 4, *infra*.

70 *See* Fla. HB 115-B First Engrossed (2001). (The Goodlette amendment is on file with the First Amendment Foundation, Tallahassee, FL.)

71 *See* Fla. HB 147-B (2001) at pp. 2 – 4.

72 Federal aircraft registration requirements can be found at http://www.faa.gov/safety/programs_initiatives/oversight/iasa/model_aviation/media/PART04.doc, or through the FAA's website, www.faa.gov.

73 Lucy Morgan and Steve Bousquet, *Florida Senate to Vote on Meeting in Secret*, St. Petersburg Times, Oct. 24, 2001.

74 *See* Fla. Senate Journal, Oct. 25, 2001, at pp. 44 – 45. The Florida House of Representatives had considered a similar rule amendment in September, 2001, but eventually abandoned the idea. *See* Joe Follick, *Lawmakers Consider Closing Meetings on State Security,* The Tampa Tribune, Sep. 27, 2001. *See also* Feeney Letter; and Letter from Representative Dan Gelber, Florida House of Representatives, to Barbara Petersen, President, First Amendment Foundation, Sep. 29, 2001. (Letters on file with the First Amendment Foundation, Tallahassee, FL.)

to the public. The constitutional provision does allow, however, for closure of meetings in those limited occasions when security is an issue:

> This section shall be implemented and defined by the rules of each house, and such rules shall control admission to the floor of each legislative chamber and may, where reasonably necessary for security purposes or to protect a witness appearing before a committee, provide for the closure of committee meetings.[75]

There were those who argued that the proposed rule allowing for closed meetings was unconstitutional, asserting that closure was allowed only when the *physical* security of the chamber or witness was required.[76] However, Article III, section 4(e) mandates that each chamber "shall be the sole judge for the interpretation, implementation, and enforcement" of the constitutional right of access to legislative meetings, thus allowing little room for an effective argument on the constitutionality of the rule change to allow for secret meetings.

The proposed rule amendment that would allow the Senate to deny access to records associated with such meetings was a different story, though. Specifically, Article I, section 24, of the State Constitution grants a right to inspect or copy all legislative records, stipulating that "[t]he legislature…may provide *by general law* for the exemption of records" from the constitutional right of access.[77] In other words, the Constitution specifically prohibited the Senate from creating an exemption for its records *by rule*.

Criticism of the proposed rule change was swift and furious, and came from an unusual assortment of disparate groups and organizations, including civil libertarians, open government advocates and-most surprisingly-the National Rifle Association.[78] Even Governor Jeb Bush said he was "troubled" that Senators would meet in secret and keep their votes shielded from the public. "This is an area we really need to be careful in how we proceed," he said.[79]

The most vocal and harshest critic, perhaps, was Senator Locke Burt, R-FL/Ormond Beach, one of only two Senators to vote against the proposed rule change in committee. In addition to arguing there was no proof that closed meetings would improve public safety, Senator Burt said, "If I wanted to raise your taxes, take away your guns, or infringe on your civil liberties, I would do it in a secret meeting. It's unnecessary, it's bad public policy, it goes against our commitment to open government and it ought to concern people."[80] The vast majority of senators, however, supported the proposal, claiming it was necessary in the wake of 9/11.[81]

The move may also have been unprecedented in a security-conscious nation. According to Brenda Erickson, a senior research analyst with the National Conference of State Legislators, in the five or six weeks following the terrorist attacks, "twenty-six states created offices of homeland se-

75 Fla. Const. Art III, § 4(e).

76 *See* Letter from Barbara Petersen, President, First Amendment Foundation, to Senator Tom Lee, Chair, Senate Rules and Calendar Committee, The Florida Senate, Oct. 23, 2001. (Letter on file with the First Amendment Foundation, Tallahassee, FL.)

77 Fla. Const. Art I, § 24(c) (emphasis added).

78 *See, e.g.,* Mark Silva, *Senate Could Act in Secret,* The Orlando Sentinel, Oct. 24, 2001; Editorial, *Security, But Not Over Freedom,* St. Petersburg Times, Oct. 24, 2001; Editorial, *Dangerous Territory*, The Daytona Beach News-Journal, Oct. 24, 2001; Thomas B. Pfankuch, *Security Measures Too Much, Too Soon?*, The Florida Times-Union, Oct. 25, 2001; David Wasson, *State Lawmakers OK Secret Senate Meetings,* The Tampa Tribune, Oct. 26, 2001; and Lesley Clark, *Senators Approve Secret Committee Meetings*, The Miami Herald, Oct. 26. 2001 [hereinafter Clark Oct. 26 Article].

79 *See* Laura Zuckerman, *Official Touts Plan to Seal Records*, The Daytona Beach News-Journal, Oct. 28, 2001 [hereinafter Zuckerman Oct. 28 Article]. *See also* Steve Bousquet, *Senate Favors Secret Meetings*, St. Petersburg Times, Oct. 25, 2001,

80 *See* Zuckerman Oct. 28 Article.

81 *See, e.g., Id.*; and Clark Oct. 26 Article.

curity, special legislative security committees or appointed security chiefs. However, the Florida Senate likely leads the way in making substantial changes to its open meetings rules."[82]

The proposed rule amendment was heard by the Senate Rules and Calendar Committee on October 24th, and the committee voted 14-to-1 to close meetings to discuss security measures, and 12-to-2 to keep all documents, including the votes of Senators, secret for as long as five years or more.[83]

The proposal went before the full Senate on October 25, 2001, which approved two changes to the records provision: First, the language specific to the votes and the substance of the votes was deleted, with the intent of making the Senators' votes public record. Second, language was added to limit the duration of the records closure, specifying that the records would be automatically subject to public disclosure thirty days after the closed meeting unless the Senate President extended the duration of the closure. No changes were made to the meetings provision.[84] Incredibly, the Senators then approved an historical and unprecedented change to its rules by voice vote, "sparing them the burden of accountability."[85]

SPECIAL SESSION 2001 C

After the flawed October special session that ended in partisan "hissy fits" and near failure, Governor Bush called the Legislature back to Tallahassee in late November to consider, once again, security and budget issues.[86] In bringing them back, however, the Governor warned legislators that he was interested only in security legislation that would support his efforts to create regional antiterrorist task forces and protect the state's pharmaceutical stockpiles. "Let's stay focused on the stuff that doesn't require heavy lifting to pass," Bush said.[87] As a result of Governor Bush's admonition, perhaps, and House Speaker Tom Feeney's reluctance "to use Sept. 11 as an excuse to ram through numerous proposals that would . . . sharply curtail[] public access to government operations."[88] Only five of the proposed exemptions considered during the first special session were re-filed during Special Session 2001 C. Four passed.[89]

---

82 *See* Jim Ash, *Proposal Criticized as Attack on Sunshine*, The Palm Beach Post, Oct. 25, 2001.

83 *See* Steve Bousquet, *Senate Favors Secret Meetings,* St. Petersburg Times, Oct. 25, 2001. As approved by the Senate Rules and Calendar Committee, records would be closed for five years but subsequent Senate Presidents could continue to seal the records every five years after that. The committee also voted to "sunset" the rule in 2003 unless, of course, future Senate presidents recommended its reenactment. "The last time I looked, terrorism didn't have a calendar. I would never vote to do away with this provision. This is a safeguard," said Senator Ron Silver, D-North Miami Beach. In fact, the rule is still in effect today. *See* §§ 1.43(1)(a) and 1.444(11), Rules and Manual of the Fla. Senate 2006 – 2008 (as adopted Nov. 21, 2006).

84 *See* Fla. Senate Journal, Oct. 25, 2001, at pp. 44 – 45. *See also* First Amendment Foundation, *Alert: Rule Change is Adopted w/Amendments; Gov Expands the Call*, Oct. 25, 2001. (FAF *Alert* on file with the First Amendment Foundation, Tallahassee, FL)

85 Editorial, *Preserve Public Access*, The Palm Beach Post, Nov. 25, 2001.

86 Executive Office of the Governor, Proclamation to the Honorable Members of the Florida Senate and the House of Representatives, Nov. 6, 2001. *See also* Roberts Nov. 4 Op-Ed.

87 *See* Wire Services, *House Panel Okays Security Bill*, The St. Petersburg Times, Nov. 29, 2001; and Bob Mahlburg, *Gov. Bush Wants Legislature to OK Basic Anti-Terrorism Bills*, The Orlando Sentinel, Nov. 29, 2001 [hereinafter Mahlburg Nov. 29 Article].

88 Orlando Sentinel Dec. 9 Editorial. *See also* Nancy Cook Lauer, *Capitol Corner: House Action on Senate Bill Quite a Rarity*, Tallahassee Democrat, Dec. 7, 2001.

89 However, all of the proposed exemptions considered during Special Session 2001 B, including those that passed in Special Session 2001-C, were filed for consideration during the regular 2002 session. All failed. Those filed for reconsideration: SB 488 and HB 729, Hospital Emergency Management Plans, SB 490 and HB 733, Pharmaceutical Materials, SB 492 and HB 741, Law Enforcement Transmittal Letters, SB 494 FDLE/Automatic Delay, HB 731 and SB 970, Aerial Applicators, HB 737, Cellular Telephone Numbers & Billing Records, and HB 739, Digital Pager Numbers & Billing Records. In addition, four security-related shell bills were filed in the Senate: SB 982, SB 984 and SB 986, Public Records/Preservation of Public Safety, and SB 1260, Public Records/Bioterrorism

Although the second special session post-9/11 was less chaotic and more focused than the preceding special session, it was not without controversy: On the opening day of Special Session 2001-C, the senate introduced twelve anti-terrorism bills outside the purview of the call, referred the bills to committee, and scheduled them for consideration. Less than three hours later, the Florida Senate Criminal Justice Committee hurriedly amended and/or approved eleven of the twelve bills - five of which created new exemptions to the public records law—and sent them to the floor for consideration by the full Senate the following day.[90] Open government advocates, angered over the lack of proper notice by the senate committee, called the short notice "stunning and completely outrageous," complaining "that the [s]enate in essence shut out the public by giving short notice that a host of public records exemption bills would be heard on the first day of a special session called to resolve a $1.3 billion budget shortfall."[91]

Of the five bills approved by the Senate committee, only four were considered by the full Senate on December 3, 2001; the most controversial bill, which would allow the FDLE to delay access to public records, was allowed to languish on the senate special order calendar.[92] The Florida House Select Committee on Security, in a rare show of legislative cooperation, then took up and approved the four Senate bills the following day. All four were passed by the House on December 5, 2001, and signed into law by Governor Bush less than a week later. Action was quick, certainly, but only those open government bills for which there was a general consensus successfully made it through the process.

Special Session 2001 C: Legislative Proposals

CS/SB 16-C Security Systems Plans

Senate Bill 16-C reenacted and slightly expanded the exemption under § 281.301, F.S., for information relating to security systems and meetings related to such information, moving the public record exemption to § 119.071[93], and the meetings exemption to § 286.0113. Section 281.301, F.S., provided an exemption for all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations revealing security systems are exempt, as are all meetings relating directly to or that would reveal such systems; SB 16-C expanded-and clarified[94] the exemption to include threat assessments, threat-response plans, emergency-evacuation plans, sheltering arrangements, or manuals for security personnel, emergency equipment, or security training.

After minor amendments were adopted, CS/SB 16-C was unanimously approved by the Florida Senate Criminal Justice Committee, and sent to the senate floor where it was further amended to make the exemption retroactive; the bill passed by a vote of 38/0. Rather than take up the house companion bill, HB 41-C, which was similar but not identical, the Florida House Select Committee

Threats. Three of the shell bills died in committee without consideration; the fourth, SB 982 was amended and its House companion, CS/HB 735 passed the Legislature. *See* First Amendment Foundation, Final Report 2002 Session, March 22, 2002. (Report on file with the First Amendment Foundation, Tallahassee, FL.)

90 *See* Mike Salinero, *Open Record Laws in Florida Remain Untouched for Now*, The Tampa Tribune, Nov. 29, 2001.

91 Lesley Clark, *Florida Takes a Step to Seal Public Records in Terror Cases*, The Miami Herald, Nov. 28, 2001.

92 The CS/SB 28-C, authorizing the FDLE to delay access to public records for as long as 21 days, was approved by the Senate Criminal Justice Committee by a vote of 5/1 (Sen. Locke Burt voting nay). *See* Fla. SB 28-C (2001). After the House made it clear that it would not consider the bill, CS/SB 28-C was allowed to die on the Senate's special order calendar. *See* Thomas B Pfankuch, *Lawmakers Ignite Anger Over Security,* The Florida Times-Union, Nov. 29, 2001; Bob Mahlburg, *New Front Opened on Terrorism*, The Orlando Sentinel, Dec. 4, 2001, and Jackie Hallifax, *Senate Squashes Effort to Seal Public Records*, The Tampa Tribune, Dec. 4, 2001.

93 Recodified as § 119.071(3)(a) (2007).

94 *See* AGO 01-75 at p. 3.

unanimously approved CS/SB 16-C, sending it for consideration by the House. The house passed CS/SB 16-C by a vote of 115 to 3. Less than a week later, the CS/SB 16-C was signed into law by the Governor.[95]

Originally scheduled for sunset review in 2006,[96] the security systems plans exemption was amended in 2003 to clarify that the security systems plans of a public or private entity *held* by an agency are exempt from public disclosure-the original language applied to those plans *possessed* by an agency. The bill, CS/SB 1182, also created an exception to the exemption, allowing disclosure of the security systems plans to the property owner or lease holder.[97]

Both the public record exemption and meeting exemption for security systems plans were reenacted in 2006 with minor, technical modifications.[98]

SB 18-C and HB 43-C, Hospital Emergency Management Plans

Senate Bill 18-C, creating a public record exemption for portions of a comprehensive emergency-management plan which address the response of a public or private hospital to an act of terrorism, including those portions addressing security systems or plans, was virtually identical to legislation filed in the previous special session. It was amended in the senate Florida Criminal Justice Committee to make the exemption retroactive and was unanimously approved. An amendment offered on the Senate floor by Senator Rod Smith, D-FL/Gainesville, to stipulate that information addressing the sufficiency of a hospital's response to an act of terrorism is *not* exempt from public disclosure, was adopted, and CS/SB 18-C passed out of the senate unanimously.

The Florida House Select Committee then took up the Senate bill rather than HB 43-C, its companion, and reported it favorably with a vote of 11/0. CS/SB 18-C was passed by a vote of 116/2 in the House and signed into law by the Governor.[99]

The exemption for hospital emergency-management plans was reenacted with modification in 2006.[100]

SB 20-C and HB 45-C, Pharmaceutical Materials

Amid growing concerns that the exemption for information identifying the types of pharmaceutical materials stockpiled by the state as part of its plan to defend against an act of terrorism was too restrictive in that it did not allow for public oversight,[101] the legislation was significantly amended by the Florida Senate Criminal Justice Committee.

As amended and approved by the committee, CS/SB 20-C allowed a public record exemption for information identifying or providing the location of the facility where pharmaceutical material was stored; any information as to the type or amount of pharmaceutical material in such storage facilities

95 Fla.Ch. No. 2001-161.

96 Under Florida law, all newly-created exemptions to the public records law and sunshine law must be reviewed and reenacted five years after original enactment or the exemption automatically "sunsets" – that is, expires. *See* § 119.15, F.S. (Open Government Sunset Review Act) (2007).

97 *See* Staff of Fla. Sen. Governmental Oversight and Productivity Committee, Analysis and Economic Impact Statement of SB 1182 (Mar. 27, 2003) at p. 3. CS/SB 1182 was passed unanimously by both chambers and signed into law by the Governor. *See* Fla. Ch. No. 2003-16. Interestingly, SB 1182, as originally drafted, repealed the now-redundant exemption under § 281.301, but the repeal language was removed by the Senate Governmental Oversight and Productivity Committee. Thus, the redundant exemption still applies. *See* Fla. Stat. § 281.301 (2007).

98 *See* Fla. Ch. No. 2006-108 (HB 7023).

99 Fla. Ch. No. 2001-362.

100 *See* Fla. Ch. No. 2006-109 (HB 7025).

101 *See* Bob Mahlburg, *Senators Go for Secrecy*, The Orlando Sentinel, Nov. 28, 2001, and Steve Bousquet, *Senate Lets Public Records Bill Die*, St. Petersburg Times, Dec. 4, 2001.

would be subject to public disclosure. In addition, the bill specifically stated that the governor's certification as to the sufficiency of the location, its contents, and capacities is public record. Finally, CS/SB 20-C was amended to allow disclosure of the exempt information to certain entities under specified circumstances.[102]

After unanimous passage in the Senate, CS/SB 20-C passed out of the House by a vote of 116/2 and was signed into law by Governor Bush.[103] The exemption was reenacted in 2006 with minor modification.[104]

SB 22-C and HB 47-C, Law Enforcement Transmittal Letters

Certainly, the least controversial bill considered during either special session, SB 22-C simply clarified existing law[105] and allowed a public record exemption for requests of law enforcement agencies to inspect or copy public records in the custody of another agency. An amendment to make the exemption remedial in nature was adopted by the Florida Senate Criminal Justice Committee, which then unanimously approved the bill. The CS/SB 22-C passed the senate by a vote of 37/1 and, after unanimous approval by the Florida House Select Committee on Security, the legislation passed the House by a vote of 117/2. Governor Bush signed the bill into law on December 10, 2001.[106]

The exemption was reenacted with minor, technical modification in 2007.[107]

102 *See* Fla. CS/SB 20-C (2001).
103 Fla. Ch. No. 2001-363. The House companion, HB 45-C, died on the House Calendar without consideration.
104 *See* Ch. No. 2006-158 (HB 7033).
105 *See* AGO 01-75 at p. 4.
106 Fla. Ch. No. 2001-364 (2001).
107 *See* Fla. Ch. 2007-93 (CS/SB 816).

SUBSEQUENT LEGISLATIVE SESSIONS 2002

In addition to the numerous exemptions originally filed during Special Session 2001-B,[108] two additional open government exemptions related to security were considered by the legislature in 2002, the first during the regular session and the second during Special Session 2002 E.

HB 735 and SB 982, Building Plans and Blueprints

As originally filed, HB 735 simply duplicated the exemption for security systems plans enacted in Special Session 2001-C.[109] A strike-all amendment by the Florida House State Administration Committee, however, created a new public record exemption for building plans, blueprints, schematic drawings, and diagrams depicting the internal layout and structural elements of buildings, arenas, stadiums, water treatment facilities, and other structures owned or operated by a government agency. As amended, the bill allowed disclosure under certain, specified circumstances or upon court order and a showing of good cause.

According to its constitutionally required statement of public necessity, the exemption was necessary to

> . . . [E]nsure public safety. Such exempt information is a vital component of public safety and if it were made publicly available, the ability of persons who desire to harm individuals located in or using those structures…would be increased. In addition, terrorists would have easy access to the exempt information and use the information to inflict harm on the public. Al-

108 *See* fn. 89.
109 *See* Staff of H.R. State Administration Committee Analysis of HB 735 (Feb. 19, 2002) at p. 5. House Bill 735 was originally filed as a proposed committee bill, PCB SEC 02-13, by the House Select Committee on Security.

> though skill would be required to use such information to further an act of terrorism, ample evidence exists of the capabilities of terrorists to conduct complicated acts of terrorism. The September 11, 2001, attack on the World Trade Center and the Pentagon, as well as the intentional spread of anthrax in the country and state, provides evidence that such capabilities exist. These events also show the crippling effect that terrorist acts can have, not only on the lives of persons in a community affected by terrorist acts but also on the economy of the community, the state, and the nation.[110]

Relatively narrow in scope and without the controversy of open government exemptions proposed in previous sessions,[111] CS/HB 735 passed the House by a vote of 101/14.

The Senate companion, SB 982, was a shell bill amended by the Florida Senate Select Committee on Security and Crisis Management, and although similar to its house companion, the senate bill, as amended, did not allow for the disclosure of the exempt information except by a showing of good cause and court order. The CS/SB 982 was tabled by the senate, however, which then substituted and passed CS/HB 735 by a vote of 33/4. The bill was subsequently signed into law by the Governor.[112]

Reviewed and reenacted without modification in 2007,[113] the exemption has just recently caused controversy-the Florida Department of Transportation refused to release state bridge inspection reports after the Minnesota bridge collapse on August 1, 2007, claiming the reports were exempt because they revealed the structural elements of the various bridges.[114] Florida law, however, stipulates that if a record contains exempt and non-exempt information, that which is exempt must be redacted and access provided to the remainder.[115] Thus, the department could not lawfully deny access to the bridge inspection reports simply because the reports contain information that is exempt from disclosure. Although the issue has yet to be resolved as of the date of this paper, summaries of the reports were ultimately released.[116]

HB 21-E and SB 24-E, Military Discharge Papers

Certainly the oddest legislation filed under the cloak of security these two companion bills, as originally filed, would allow a public record exemption for all identifying information contained in a U.S. military discharge record held by the clerk of court.

Historically, the U.S. Department of Defense (DoD) had advised those discharged from the military to record their separation documents with their local clerk of court where such documents would become part of the official records of the county.[117] However, as clerks of court in Florida placed official records on the Internet,[118] concern arose about the specter of identify theft and the possible illicit use of personal information contained in military discharge records, and the DoD began advising individuals otherwise.[119] In addi-

110 Fla. CS/HB 735 (2001).

111 *See* Letter from Barbara Petersen, President, First Amendment Foundation, to Representative Fred Brummer, Florida House of Representatives, Feb. 14, 2002. (Letter on file with the First Amendment Foundation, Tallahassee, FL.)

112 Fla. Ch. No. 2002-67.

113 *See* fn. 93 and Fla. Ch. No. 2007-95 (SB 886).

114 *See, e.g.,* Jim Ash, *Lawmaker Seeks Release of Bridge Inspection Reports*, The Tallahassee Democrat, Aug. 17, 2007, and Paige St. John, *Florida Bridge Inspection Reports to Go Public*, The News-Press, Aug. 17, 2007 [hereinafter St. John Aug. 17 Article].

115 Fla. Stat. § 119.07(1)(b) (2007).

116 *See* St. John Aug. 17 Article.

117 Staff of Fla. H.R. State Administration Committee Analysis of HB 21-E (Apr. 30, 2002) at p. 1 [hereinafter Staff Analysis of HB 21-E].

118 Section 28.2221, F.S., required clerks of court to make copies of all official records available on the county's official website. Any military discharge document recorded with the clerk of court would be included in those official records required to be posted to the Internet.

119 Staff Analysis of HB 21-E. Personal information contained in a military discharge record includes names,

tion to justifying the proposed exemption for the purpose of thwarting identity theft, though, the public necessity statements in both bills took it a step further and incredibly attempted to justify the exemption in the name of *security*:

> The legislature finds that exempting personal identifying information contained in military separation forms is a public necessity because the availability of that information in public records, especially when accessible on the Internet, facilitates the crime of identity theft and permits the identification of specific individuals who have served in the armed forces, *which information may be of use in planning for terrorist acts…[G]iven the increased threat of terrorism* in the United States *and the large number of military personnel who retire in Florida, terrorists could use the information to identity and target former military personnel and use such information in planning terrorist acts*. For example, terrorists may seek to avoid an area with a large concentration of former military personnel because those individuals may be armed and, given their military training, could threaten the success of a terrorist action. In the alternative, terrorists could seek to target a neighborhood with a large number of military retirees to seek revenge against persons who have been in the frontline of United States military actions.[120]

The legislation raised a number of serious constitutional issues, among them the question whether an exemption for information readily available from other public sources-in this specific case, military discharge records are subject to disclosure under the federal Freedom of Information Act-can be constitutionally justified as "necessary" to accomplish any valid purpose under Florida's constitution.[121]

Ultimately, both bills were amended, stripping out the exemption language, and instead, in pertinent part, allowing a veteran or the veteran's representative to request that his or her military discharge record be removed from the official records. The CS/HB 21-E was tabled, and its companion, SB 24-E, was passed unanimously by both the Senate and the House as amended, and signed into law by the governor.[122]

2004

HB 317 and SB 410, Building Plans and Blueprints of Privately-Owned Structures

Only one security-related open government exemption was considered during the 2004 legislative session. It was an exemption that would extend the protection for building plans and blueprints, etc., would allow for government-owned structures to include building plans and blueprints of certain privately-owned facilities and structures *held* by an agency. Again, the concern was public safety and the breadth of Florida's public records

social security numbers, dates of birth, homes of record, and next of kin. Id.

120 Fla. HB 21-E at pp. 1 – 3 and Fla. SB 24-E at pp. 1 – 3 (emphasis added).

121 *See* Letters from Barbara Petersen, President, First Amendment Foundation, to Representative Jerry Paul, Florida House of Representatives, Apr. 30, 2002 (HB 21-E) and Senator Ginny Brown-Waite, Florida Senate, Apr. 30, 2002 (SB 24-E) [hereinafter Military Discharge Record Letters]. (Letters on file with the First Amendment Foundation, Tallahassee, FL.) In addition, the Legislature passed a bill during the 2002 regular session, HB 1679, which required the clerks of court to remove a military discharge record from the Internet if requested to do so by the subject of the record. *See* Fla. Ch. No. 2002-302. The FAF took the position that removing such records from the Internet upon request addressed the concerns of the military veterans without offending the public's constitutional right of access – such records would be available pursuant to a public record request to the clerk of court even though no longer available on the Internet. *See* Military Discharge Record Letters.

122 Fla. Ch. No. 2002-391. Because the bill did not technically create a public record exemption, it is not subject to the Open Government Sunset Review Act.

law—a blueprint of a privately-owned theme park, for example, provided to a government agency becomes subject to public disclosure under Florida law absent a specific statutory exemption.

As filed, the two companion bills were virtually identical, each providing a public record exemption for building plans, blueprints, schematic drawings, and diagrams which depict the internal layout or structural elements of an attractions and recreation facility, entertainment or resort complex, industrial complex, retail and service development, office development, or hotel or motel development, which were held by a government agency. Each of the different types of protected complexes and developments were specifically and carefully defined in the legislation. The legislation also allowed for disclosure to other governmental entities when necessary to the performance of its duties and responsibilities, to the owner or owners of the structure in question, or upon court order and a showing of good cause.[123] Finally, each bill was amended in committee to stipulate that the proposed exemption did *not* apply to comprehensive plans or site plans submitted for approval under local land use regulations, thus allowing the public access to such plans prior to approval by local government.[124]

There was little opposition to the proposed exemption, and CS/HB 317 passed the House by a vote of 113/3. After tabling its own bill, the senate passed the house bill by a vote of 39/1, and it was signed into law by Governor Bush. The exemption is scheduled for open government sunset review in 2009.[125]

123 *See* Fla. HB 317 and SB 410 (2004).
124 *See* Fla. CS/HB 317 *and* CS/SB 410.
125 Fla. Ch. No. 2004-9.

2005

SB 1416 and HB 1801, Meetings/Domestic Security Oversight Council

Although security-related legislation was filed during the 2005 regular session, there was only one new exemption proposed[126]-an exemption for the newly codified Domestic Security Oversight Council.[127]

Nearly identical, SB 1416 and HB 1801 would create a narrow exemption for portions of meetings of the Domestic Security Oversight Council at which the council would hear and/or discuss active criminal investigative or intelligence information. The legislation contained a number of limitations: first, the council chair must announce at a public meeting the need to discuss such information in connection with the performance of the council's duties; second, the chair must declare, in writing, the specific reasons closure is necessary, and file the document-as a public record-with the official documents of the council; third, the entire closed meeting must be recorded; and fourth, attendance at the closed meeting would be strictly

126 During the 2005 session, the Legislature reenacted § 311.13, F.S., providing an exemption for seaport security plans, pursuant to the Open Government Sunset Review Act and without modification. *See* Fla. SB 288 (2005). The bill passed both houses unanimously and was signed into law by Governor Bush. *See* Fla. Ch. No. 2005-53. Because the exemption was originally enacted in 2000 – prior to the terrorist attacks of 9/11 – it was not included in this paper. In addition, one shell bill, SB 1226, expressing legislative intent to revise laws related to domestic security was filed; the bill was not considered and died in its first committee of reference. *See* Fla. SB 1226 (2005).

127 *See* E-mail from Barbara Petersen, President, First Amendment Foundation, to Bill Garner, Staff Attorney, Committee on Domestic Security, Florida House of Representatives, Mar. 10, 2005. (E-mail on file with the First Amendment Foundation, Tallahassee, FL.) According to Mr. Garner, the Domestic Security Oversight Council was designed to coordinate the work of the state's regional domestic security task forces and state working groups in "defining domestic security and counter-terrorism funding recommendations that are made to the Governor and Legislature."

limited. The legislation also contained an exemption for records generated during the closed meeting, stipulating that such records would be subject to disclosure once the criminal investigation or intelligence information ceased to be active.

Again, there was very little debate over the merits of the proposed exemption, and the only real issue was which version was preferable-the House or the Senate.[128] After minor committee amendments, HB 1801 was passed unanimously out of the House. The Senate tabled its companion bill, substituted the House bill and passed it unanimously as well. The legislation was signed into law by Governor Bush.[129]

CONCLUSION

After the panicked response of the Florida legislature in the immediate aftermath of 9/11 and the discovery of anthrax in South Florida, it seemed entirely possible at the time that the legislature would do serious harm to the people's constitutional right of access to their government, rolling back open government protections and public policy that had been in place for over a hundred years.

But something happened between the first special session in October 2001 and the second in November—the entire legislative body appeared to take a deep collective breath and, with a fresh eye, considered which of the plethora of proposed new exemptions were truly necessary to protect the security of the state and the safety of its citizens. As a result, only four new open government exemptions were created in the two special sessions called by the governor to deal with security issues, and an equal number have been created in subsequent legislative sessions. All are arguably narrow and sufficiently specific so as to meet the constitutional standard.

Ultimately, it took the collective effort of the governor, the legislature and legislative staff, the media, civil libertarians, open government advocates, and governmental watchdogs, to craft sensible, prophylactic, and most significantly, constitutional legislation meant to enhance the safety and security of the state and its citizens without eroding the vital and historic principals of access to government.

SUMMARY OF SECURITY-RELATED OPEN GOVERNMENT LEGISLATION PASSED IN RESPONSE TO 9/11

2001

Section 119.071(3)(a), F.S., Security Systems Plans Records[130]

1. As used in this paragraph, the term "security system plan" includes all:
   a. Records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to the physical security of the facility or revealing security systems;
   b. Threat assessments conducted by any agency or any private entity;
   c. Threat response plans;
   d. Emergency evacuation plans;
   e. Sheltering arrangements; or
   f. Manuals for security personnel, emergency equipment, or security training.

2. A security system plan or portion thereof for:
   a. Any property owned by or leased to the state or any of its political subdivisions; or
   b. Any privately owned or leased property held by an agency is confidential and exempt from § 119.07(1) and § 24(a), art. I

128 *See* Petersen/Garner E-mail.

129 Fla. Ch. No. 2005-211.

130 *See* Fla. CS/SB 16-C (Ch. No. 2001-361) (2001), available at http://www.flsenate.gov/session/index.cfm?BI_Mode=ViewBillInfo&Mode=Bills&SubMenu=1&Year=2001C&billnum=16-C.

of the State Constitution. This exemption is remedial in nature, and it is the intent of the Legislature that this exemption apply to security system plans held by an agency before, on, or after the effective date of this paragraph.

3. Information made confidential and exempt by this paragraph may be disclosed by the custodian of public records to:
   a. The property owner or leaseholder; or
   b. Another state or federal agency to prevent, detect, guard against, respond to, investigate, or manage the consequences of any attempted or actual act of terrorism, or to prosecute those persons who are responsible for such attempts or acts.

Section 286.0113(1), F.S., Security Systems Plans Meetings[131]

That portion of a meeting that would reveal a security system plan or portion thereof made confidential and exempt by § 119.071(3)(a) is exempt from § 286.011 and § 24(b), art. I of the State Constitution.

Section 395.1056, F.S., Hospital Emergency Management Plans[132]

(1)(a) Those portions of a comprehensive emergency management plan that address the response of a public or private hospital to an act of terrorism as defined by § 775.30 held by the agency, a state or local law enforcement agency, a county or municipal emergency management agency, the Executive Office of the Governor, the Department of Health, or the Department of Community Affairs are confidential and exempt from § 119.07(1) and § 24(a), Art. I of the State Constitution.

(b) Information made confidential and exempt by this subsection may be disclosed by a custodial agency to another state or federal agency to prevent, detect, guard against, respond to, investigate, or manage the consequences of any attempted or actual act of terrorism, or to prosecute those persons who are responsible for such attempts or acts.

(c) Portions of a comprehensive emergency management plan that address the response of a public or private hospital to an act of terrorism include those portions addressing:
   1. Security systems or plans;
   2. Vulnerability analyses;
   3. Emergency evacuation transportation;
   4. Sheltering arrangements;
   5. Post disaster activities, including provisions for emergency power, communications, food, and water;
   6. Post disaster transportation;
   7. Supplies, including drug caches;
   8. Staffing;
   9. Emergency equipment; and
   10. Individual identification of residents, transfer of records, and methods of responding to family inquiries.

(2) Those portions of a comprehensive emergency management plan that address the response of a public hospital to an act of terrorism as defined by § 775.30 held by that public hospital are exempt from § 119.07(1) and s. 24(a), art. I of the State Constitution. Portions of a comprehensive emergency management plan that address the response of a public hospital to an act of terrorism include those portions addressing:
   (a) Security systems or plans;
   (b) Vulnerability analyses;
   (c) Emergency evacuation transportation;
   (d) Sheltering arrangements;
   (e) Post disaster activities, including provi-

131 *Id.*

132 *See* Fla. CS/SB 18-C (Ch. No. 2001-362) (2001), available at http://www.flsenate.gov/session/index.cfm?BI_Mode=ViewBillInfo&Mode=Bills&SubMenu=1&Year=2001C&billnum=18.

sions for emergency power, communications, food, and water;
(f) Post disaster transportation;
(g) Supplies, including drug caches;
(h) Staffing;
(i) Emergency equipment; and
(j) Individual identification of residents, transfer of records, and methods of responding to family inquiries.

(3) The public records exemptions provided by this section are remedial in nature, and it is the intent of the Legislature that the exemptions apply to plans held by a custodial agency before, on, or after the effective date of this section.

(4) That portion of a public meeting which would reveal information contained in a comprehensive emergency management plan that addresses the response of a hospital to an act of terrorism is exempt from § 286.011 and § 24(b), Art. I of the State Constitution.

(5) The certification by the governor, in coordination with the Department of Health, of the sufficiency of a comprehensive emergency management plan that addresses the response of a hospital to an act of terrorism is not exempt.

Section 381.95, F.S., Pharmaceutical Materials[133]

(1) Any information identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities, or laboratories established, maintained, or regulated by the Department of Health as part of the state's plan to defend against an act of terrorism as defined in § 775.30 is exempt from § 119.07(1) and § 24(a), Art. I of the State Constitution. This exemption is remedial in nature, and it is the intent of the Legislature that this exemption apply to information held by the Department of Health before, on, or after the effective date of this section.

(2) Information made exempt by this section may be disclosed by the custodial agency to another state or federal agency in order to prevent, detect, guard against, respond to, investigate, or manage the consequences of any attempted or actual act of terrorism, or to prosecute those responsible for such attempts or acts.

(3) The certification by the Governor of the sufficiency of any location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities, or laboratories established, maintained, or regulated by the Department of Health as part of the state's plan to defend against an act of terrorism is a public record.

Section 119.071(2)(c)2., F.S., Law Enforcement Transmittal Letters[134]

2. A request made by a law enforcement agency to inspect or copy a public record that is in the custody of another agency and the custodian's response to the request, and any information that would identify whether a law enforcement agency has requested or received that public record are exempt from § 119.07(1) and § 24(a), Art. I of the State Constitution, during the period in which the information constitutes active criminal intelligence information or active criminal investigative information.

133 *See* Fla. CS/SB 20-C (Ch. No. 2001-363) (2002), available at http://www.flsenate.gov/session/index.cfm?Mode=Bills&SubMenu=1&BI_Mode=ViewBillInfo&BillNum=20&Year=2001C&Chamber=Senate.

134 *See* Fla. CS/SB 22-C (Ch. No. 2001-364), available at http://www.flsenate.gov/session/index.cfm?Mode=Bills&SubMenu=1&BI_Mode=ViewBillInfo&BillNum=22&Year=2001C&Chamber=Senate.

2002

Section 119.071(3)(b), F.S., Building Plans & Blueprints Public Buildings[135]

1. Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency are exempt from § 119.07(1) and § 24(a), Art. I of the State Constitution.
2. This exemption applies to building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency before, on, or after the effective date of this act.
3. Information made exempt by this paragraph may be disclosed:
   a. To another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities;
   b. To a licensed architect, engineer, or contractor who is performing work on or related to the building, arena, stadium, water treatment facility, or other structure owned or operated by an agency; or
   c. Upon a showing of good cause before a court of competent jurisdiction.
4. The entities or persons receiving such information shall maintain the exempt status of the information.

135 *See* Fla. CS/HB 735 (Ch. No. 2002-67) (2002), available at http://www.flsenate.gov/session/index.cfm?BI_Mode=ViewBillInfo&Mode=Bills&SubMenu=1&Year=2002&billnum=735.

Section 295.186, F.S., Military Discharge Records[136]

Any veteran of the United States Armed Forces or his or her widow or widower, attorney, personal representative, executor, or court appointed guardian has the right to request that a county recorder remove from the official records any of the following forms recorded before, on, or after the effective date of this act, by or on behalf of the requesting veteran: DD-214; DD-215; WD AGO 53; WD AGO 55; WD AGO 53-55; NAVMC 78-PD; and NAVPERS 553. The request must specify the identification page number of the form to be removed. The request shall be made in person and with appropriate identification to allow determination of the identity of the requested. The county recorder has no duty to inquire beyond the request to verify the identity of the person requesting the removal. No fee shall be charged for the removal. When the request for removal is made, the county recorder shall provide a written notice to the requesting party that the removal of the document from the official records is permanent and no further record of the document will exist in the official records of the county.

2004

Section 119.071(3)(c), F.S., Building Plans & Blueprints Private Facilities[137]

136 *See* Fla. SB 24-E (Ch. No. 2002-391) (2002), available at http://www.flsenate.gov/session/index.cfm?BI_Mode=ViewBillInfo&Mode=Bills&SubMenu=1&Year=2002E&billnum=24.

137 *See* Fla. CS/HB 317 (Ch. No. 2004-9) (2004), available at http://www.flsenate.gov/session/index.cfm?BI_Mode=ViewBillInfo&Mode=Bills&SubMenu=1&Year=2004&billnum=317. Although the sunset review language is not included in the statutory, a to § 119.071(3)(c) states: Note.--Section 2, ch. 2004-9, provides that "[s]ection [119.071(3)(c)], Florida Statutes, is subject to the Open Government Sunset Review Act of 1995, in accordance with§ 119.15, Florida Statutes, and shall stand repealed on October 2, 2009, unless reviewed and reenacted by the Legislature."

Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout or structural elements of an attractions and recreation facility, entertainment or resort complex, industrial complex, retail and service development, office development, or hotel or motel development, which documents are held by an agency are exempt from § 119.07(1) and § 24(a), Art. I of the State Constitution. This exemption applies to any such documents held by an agency before, on, or after the effective date of this act. Information made exempt by this paragraph may be disclosed to another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities; to the owner or owners of the structure in question or the owner's legal representative; or upon a showing of good cause before a court of competent jurisdiction. As used in this paragraph, the term:

1. "Attractions and recreation facility" means any sports, entertainment, amusement, or recreation facility, including, but not limited to, a sports arena, stadium, racetrack, tourist attraction, amusement park, or pari-mutuel facility that:
   a. For single-performance facilities:
      (I) Provides single-performance facilities; or
      (II) Provides more than 10,000 permanent seats for spectators.
   b. For serial-performance facilities:
      (I) Provides parking spaces for more than 1,000 motor vehicles; or
      (II) Provides more than 4,000 permanent seats for spectators.

2. "Entertainment or resort complex" means a theme park comprised of at least 25 acres of land with permanent exhibitions and a variety of recreational activities, which has at least 1 million visitors annually who pay admission fees thereto, together with any lodging, dining, and recreational facilities located adjacent to, contiguous to, or in close proximity to the theme park, as long as the owners or operators of the theme park, or a parent or related company or subsidiary thereof, has an equity interest in the lodging, dining, or recreational facilities or is in privity therewith. Close proximity includes an area within a 5-mile radius of the theme park complex.

3. "Industrial complex" means any industrial, manufacturing, processing, distribution, warehousing, or wholesale facility or plant, as well as accessory uses and structures, under common ownership which:
   a. Provides onsite parking for more than 250 motor vehicles;
   b. Encompasses 500,000 square feet or more of gross floor area; or
   c. Occupies a site of 100 acres or more, but excluding wholesale facilities or plants that primarily serve or deal onsite with the general public.

4. "Retail and service development" means any retail, service, or wholesale business establishment or group of establishments which deals primarily with the general public onsite and is operated under one common property ownership, development plan, or management that:
   a. Encompasses more than 400,000 square feet of gross floor area; or
   b. Provides parking spaces for more than 2,500 motor vehicles.

5. "Office development" means any office building or park operated under common ownership, development plan, or management that encompasses 300,000 or more square feet of gross floor area.

6. "Hotel or motel development" means any hotel or motel development that accommodates 350 or more units.

This exemption does not apply to comprehensive plans or site plans, or amendments thereto, which are submitted for approval or which have been approved under local land development regulations, local zoning regulations, or development-of-regional-impact review.

2005

Section 943.0314, F.S., Domestic Security Oversight Council[138]

(1)(a) That portion of a meeting of the Domestic Security Oversight Council at which the council will hear or discuss active criminal investigative information or active criminal intelligence information as defined in § 119.011 is exempt from § 286.011 and § 24(b), Art. I of the State Constitution, if:

1. The chair of the council announces at a public meeting that, in connection with the performance of the council's duties, it is necessary that active criminal investigative information or active criminal intelligence information be discussed.
2. The chair declares the specific reasons that it is necessary to close the meeting, or portion thereof, in a document that is a public record and filed with the official records of the council.
3. The entire closed meeting is recorded. The recording must include the times of commencement and termination of the closed meeting or portion thereof, all discussion and proceedings, and the names of the persons present. No portion of the closed meeting shall be off the record. The recording shall be maintained by the council.

(b) An audio or video recording of, and any minutes and notes generated during, a closed meeting of the council or closed portion of a meeting of the council are exempt from § 119.07(1) and § 24(a), Art. I of the State Constitution until such time as the criminal investigative information or criminal intelligence information heard or discussed therein ceases to be active. Such audio or video recording and minutes and notes shall be retained pursuant to the requirements of § 119.021.

(2) Only members of the council, staff supporting the council's functions, and other persons whose presence has been authorized by the chair of the council shall be allowed to attend the exempted portions of council meetings. The council shall ensure that any closure of its meetings as authorized by this section is limited so that the policy of this state in favor of public meetings is maintained.

(3) This section is subject to the Open Government Sunset Review Act of 1995 in accordance with § 119.15 and shall stand repealed on October 2, 2010, unless reviewed and saved from repeal through reenactment by the Legislature.

138 *See* Fla. HB 1801 (Ch. No. 2005-211), available at http://www.flsenate.gov/session/index.cfm?BI_Mode=ViewBillInfo&Mode=Bills&SubMenu=1&Year=2005&billnum=1801.

Chapter 2

Critical Infrastructure

Synopsis

2.1 *The Water Balance* by Thomas Collins
2.2 *State Laws Regarding Critical Infrastructure* by James W. Conrad, Jr.
2.3 *Exempting Critical Infrastructure Information: More Harm Than Good* by Harry Hammit
2.4 *Protecting Sensitive Information: Critical Infrastructure at the Local Level* by Maeve Dion
2.5 *Protecting Sensitive Information: A Private Sector Perspective* by Maeve Dion

2.1 The Water Balance

by Thomas Collins

The Water Balance

The water balance is an accounting of the inputs and outputs of water.

—C. W. Thornthwaite (1899–1963)

The *Water Balance* analogy is not appropriate, but in a metaphorical sense, the balance between freedom of information and restricting public access to water utility information becomes meaningful after events of September 11, 2001. The original assumption of freedom of information in public agencies is expressed by James Madison, "A popular government without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy, or perhaps both . . . a people which mean to be their own governors must arm themselves with the power which knowledge gives" (Gaillard Hunt ed. 1910). Conversely, a terrorist group with the means of acquiring popular information can arm themselves with the power which knowledge gives and it is a prologue, not to a farce, but to a singular tragedy. This paper will briefly discuss the legal actions taken by stakeholders in the critical infrastructure *water utility* after September 11, 2001 to protect Vulnerability Assessments (VA) and Emergency Response Plans (ERP) required by the *Bioterrorism and Response Act*, 2002. The paper will also analyze the current status of exemptions to the Freedom of Information Act (FOIA) regarding water related systems, where the current balance now lies, and how the States will continue toward more restrictions, not less, concerning the FOIA and potable water production (USA Patriot Act, 2002).

The Bioterrorism Act

In 2002, Congress passed the *Public Health Security and Bioterrorism Preparedness and Response Act* (Public Law 107-188) known as the Bioterrorism Act. The Act required certain drinking water systems to conduct vulnerability assessments and update their Emergency Response Plans. The Act amended the Safe Drinking Water Act to require community water systems serving populations of greater than 3,300 persons to conduct antiterrorism water Vulnerability Assessments (VA) and develop a water system Emergency Response Plan (ERP), incorporating the findings of the VAs into the ERPs. As Shermer noted there are no mandatory requirements for security upgrades in the Act (2006, p. 40). The Bioterrorism Act exempts the Safe Drinking Water Act (SDWA) vulnerability assessments from release through FOIA, and leaves the state FOIA laws to be amended through individual legislation (Altera, 2007). In Altera's analysis in the *Air Force Law Review, g*enerally the federal laws do not supersede State FOIA laws (2007, p. 14). As a result, drinking water utilities will likely not be able to rely on the FOIA exemp-

tion in the Bioterrorism Act for protecting access to all relevant water utility information at the state levels (Altera, 2007, p. 14 note 120, *supra*).

Openness, not secrecy, had been the purview of the public regarding water information, and water information had been routinely disseminated, subject to FOIA rules, under the Community-Right-to-Know-Act and the Safe Drinking Water Act. Prior to the passage of the Bioterrorism Act opinions varied regarding the historical use of the FOIA and the impact the Bioterrorism Act would have on the community's right to know. The Houston Chronicle editorial warned of the possible dangers to the community right to know if the Bioterrorism Act became law (July 2002). The Denver Post contributed to the debate by offering as an explanation the restrictions in the Bioterrorism Act may be a shield for agencies to keep secret and deny the release of *routine information*. "American lives can be negatively affected by a law that hides and limits information. Details regarding the safety of roads and bridges, railroads, food and *drinking water* could be hidden from the public" (Nov. 2002).

Routine information had not been defined, but disregarding the notion that seldom does routine information negatively impact American lives when it concerns drinking water, and rare is the *lack* of information regarding the failure of bridges *ex post facto*, the Denver Post and Houston Chronicle editorials highlighted a debate that began prior to the passage of the Bioterrorism Act in 2002 and continues to the present. In the Neimans Report (2004), Joseph Davis' response to less FOIA information about energy infrastructure hazards echoed this need for more information, not less, in an era of terrorism. Dahl (2004) calls it the "Battle for Access" and understands the philosophy of openness prior to September 11, 2001, dramatically changed, tilting the balance from openness to secrecy concerning environmental issues. By May 2002, President Bush signed Executive Order #12958, delegating the administrator of the EPA "original classification authority." Both Presidents Clinton and Bush greatly strengthened government officials' powers to classify information, but as Dahl points out, President Bush's Executive Order #13292, which amended a 1995 order by former president Bill Clinton, marked a new policy on classification of information. The Clinton Executive Order can be summarized as "when in doubt, don't classify," whereas the Bush Executive Order reversed this presumption to "when in doubt, classify" (Dahl, 2004).

By August 2002, eleven months after the tragedy of September 11, 2001, the Association of Metropolitan Water Agencies (AMWA) published *State FOIA Laws: A Guide to Protecting Sensitive Water Security Information* (AMWA, 2002). That publication provided information, background material and suggested language for model legislation for water utilities to take to their respective legislatures for quick action; the primary concern being a greater vulnerability had been created by collecting the vulnerabilities for water utilities without the states offering commensurate protection through amendments to state laws. A comprehensive review of the current status of exemptions to the FOIA related to environmental documents has been undertaken by Altera (2007) in the *Air Force Law Review*. According to Altera, the Vulnerability Assessments are not subject to FOIA requests, and they are specifically exempted through the SDWA, stating that "no community water system shall be required under State or local law to provide a vulnerability assessment to any State, regional, or local governmental entity solely by reason of the requirement set forth in paragraph (2) that the system submit such assessment to the Administrator" (Aug. 2007). Her analysis of the FOIA concluded that individual requests for information would be decided on a case by case basis.

By September, 2003, the AMWA published another set of guidelines for water utilities, this time offering legislative language and the current status of state laws regarding the water utility industry and FOIA. In *State Laws Protecting Water Security Information,* AMWA published excerpts of the state statues enacted in 2002 and 2003 to protect information that could be used to disrupt a

drinking water system. The report showed twenty-seven states passed legislation exempting certain security information, however, only ten states had language in the exemptions that specifically covered the release of information on water systems (Sept. 2003). Conflicting analysis by the National Conference of State Legislatures (NCSL) showed forty-six states appeared to have legislation exempting from public disclosure water security system information (*Protecting Water System Security Information*, NCSL, 2003). Figure 1 displays the states that have legislation exempting vulnerability assessments, including the District of Columbia; although the NCSL report showed thirty-six states having specific exemptions, the wording of the statutes are not consistent, and the report relied on the language in the statutes referring to the vulnerability assessments that are not considered to be public record (NCLS, p.2, 2003). Ten additional states provide for FOIA exemption if federal or state laws require protection of information. Those states are: Hawaii, Illinois, Indiana, Kentucky, Mississippi, New York, Pennsylvania, Utah, Vermont and Wisconsin.

Figure 1
States/Jurisdictions That Have Vulnerability Assessment Exemptions

Alaska	Missouri
Arizona	Montana
Arkansas	Nebraska
California	Nevada
Colorado	New Hampshire
Connecticut	New Jersey
Delaware	New Mexico
District of Columbia	North Carolina
Florida	North Dakota
Georgia	Ohio
Idaho	Oklahoma
Iowa	Oregon
Kansas	Rhode Island
Louisiana	Tennessee
Maine	Texas
Maryland	Virginia
Massachusetts	Washington
Michigan	West Virginia
	Wyoming

Source: *Protecting Water System Security Information,* National Conference of State Legislatures, Atkins, C., Morandi, L., 2003.

As reported in *State Open Government Law and Practice in a Post-9/11 World,* by 2007, forty-five states and the District of Columbia now have exemptions or restrictions on public information laws relating to the *specific* category of Critical Infrastructure (Aug. 2007). This is an indication that more specific restrictions are being developed for water utilities throughout the country.

Figure 2
States/Jurisdictions That Have Vulnerability Assessment Exemptions Relating to Critical Infrastructures

Alabama	Montana
Alaska	Nebraska
Arizona	Nevada
Arkansas	New Hampshire
California	New Jersey
Colorado	New Mexico
Connecticut	New York
Delaware	North Carolina
District of Columbia	North Dakota
Florida	Ohio
Georgia	Oklahoma
Idaho	Oregon
Illinois	Pennsylvania
Indiana	Rhode Island
Iowa	South Carolina
Kansas	Tennessee
Kentucky	Texas
Louisiana	Utah
Maine	Vermont
Maryland	Virginia
Massachusetts	Washington
Michigan	West Virginia
Missouri	Wyoming

Source: *State Open Government and Practice in a Post-9/11 World,* Editors: Dalglish, L.A., Cochran, L.A., Winegar, N., 2007.

Additionally, *State Open Government and Practice in a Post-9/11 World*, reported twenty-two states with specific references to water utility systems, water distribution lines, dams, or water related functions in their State exemption laws compared to exemption laws in 2003. Figure 3 lists the twenty-two states that have included specific references to water utility systems, water distribution lines, dams, or water related functions being exempted from FOIA laws at the state level. The finding indicates restrictions specifically targeting water systems in critical infrastructure are being implemented and will continue throughout the country as awareness is raised among state political leaders and water stakeholders.

Figure 3
States/Jurisdictions That Have Exemptions Specific to Water Relating to Critical Infrastructures (2007).

Arizona	Michigan
Arkansas	Nevada
California	North Dakota
Connecticut	Oklahoma
Florida	Oregon
Georgia	Tennessee
Illinois	Texas
Indiana	Utah
Iowa	Virginia
Kansas	West Virginia
Kentucky	Wyoming

Source: *State Open Government and Practice in a Post-9/11 World,* Editors: Dalglish, L.A., Cochran, L.A., Winegar, N., 2007.

In Texas this is most readily discerned through the two Attorney's General opinions over four and a half years of rulings on open records requests. In years 2003 to 2007 there have been 14 Open Records requests for information on water related utilities, and two different Attorneys General have, in all of the opinions, ruled in favor of the utilities seeking to protect sensitive information (Department of State Health Services, Office of General counsel, May 15, 2007).

The Allegorical Balancing Act: Does It Matter?

James Madison's world view: Open disclosure of information makes water utility actions transparent and is good for public health and safety; this hypothesis is based upon the assumption that agencies need prodding to produce information for general public consumption, and that agency heads, knowing such legislative prods exists will act in their own best interests, or the people who govern will replace them; openness serves the public health and safety, and carried to the logical end, national security.

> Implicit . . . in current debates in the United States is the polarization of those interested in protecting the nation and those assumed to be against such societal protection because they value individual liberties more. Yet, a summary of the arguments for access…is that this is what national security is all about. An informed citizenry is the bulwark of open government, not an inconvenience to be tolerated or a gadfly to be shooed away when government has more important matters to attend to (Strenz, 2004).

Applying C. W. Thornthwaite's *Water Balance* allegory, assume in a pre-September 11, 2001, world all public information regarding water utilities ***is*** readily available and the educated citizenry obtain it by using their respective state FOIA laws -- a balance between the public's right to know and public health and safety therefore exists. The FOIA model, ala Strenz, is in place and operating. Assume also the regulated U.S. water industry sets a high standard for water quality emulated around the world.

> America's high quality of public water supplies has traditionally been a source of local and national pride. Travelers drink water from the tap wherever they may be, with no question of its safety. Conformance to federally mandated drinking water quality standards has virtually eliminated the occurrence of waterborne diseases in this country; such diseases are not the serious problems that they are elsewhere in the world (Pontius, F. W., and Clark, S. W., p. 4, 1999).

The water industry in the United States consistently produces a standard of potable water that can be used with confidence among the citizenry traveling between the fifty states. In other countries water utilities use the United States model for water filtration, purity and quality as a benchmark for measurable achievement.

Yet, infrastructure neglected is infrastructure in danger of collapse, and as a self-inflicted wound, is capable of causing as much or more damage as a terrorist attack. As Shermer writes:

> From a relative risk standpoint, debating the likelihood and consequences of terrorist threats to drinking water infrastructure may seem like a misguided exercise. The risk terrorism poses to drinking water safety almost indisputably pales in comparison to the threats drinking water supplies face everyday from pollution, overuse, and lack of adequate funding for infrastructure maintenance. The unfortunate truth is that plenty of bad stuff gets into our drinking water already.
>
> Thousands of illnesses and hundreds of deaths occur each year, not as the result of terrorist efforts, but because of commonly-found waterborne contaminants (2006, p. 30).

This is a serious indictment, yet in 1993 a citizen requesting information concerning the Milwaukee Water Utility could make the requests for the Utility's water filtration system and it would be granted. The Milwaukee Water Utility possessed a

good record for water quality and was not in violation of the federal drinking water regulations in place at the time. All is right with the FOIA world and balance is achieved -- requests for information as inputs equal release of information as outputs. However:

> Despite this generally good record, water utilities using conventional treatment are not immune from waterborne-disease outbreaks . . . The most notable occurrence is the 1993 outbreak in Milwaukee, Wisconsin, where over 400,000 people were sickened with severe gastrointestinal upset due to cryptosporidiosis. Over 4,000 people were hospitalized, and, tragically, it is estimated that between 50 and 100 people died as a result of this illness . . . *Of particular interest to water utility professionals is the fact that at no time during the Milwaukee outbreak did the utility violate any of the federal drinking water regulations in place at that time* (Pontius, F. W., and Clark, S. W., p.4, emphasis added).

This seems to run counter to the argument that openness serves the public interests, protects public health and safety, and further, national security. At the time of the deaths of the 100 individuals the FOIA and Community Right to Know Act, and the Safe Drinking Water Act were in place. The Milwaukee cryptosporidium incident should not have occurred, yet it did even though safeguards and information sharing were in place.

An event of the magnitude of the Milwaukee poisonings raises citizen alarm, destroys confidence, endangers fears, and is costly. The costs for replacing the Milwaukee water system exceeded $100 million (Blair, 2003). The medical costs of the Milwaukee illness exceeded $67 million (Blair, 1993). Yet incidents of cryptosporidium illnesses stemming from a water utilities' inability to properly filtrate and monitor regularly occur; as late as 2005 even after the release of all available information on the causes of the Milwaukee incident people are sickened from cryptosporidium in drinking water systems (Utility Week, 2006).

The impact of the cryptosporidium tragedy resulted in amendments to the Safe Drinking Water Act regarding the monitoring and treatment of water to protect public health and safety and have now been promulgated in the Code of Federal Regulations (Ternus, M., Sept. 1995). Those interested (other than people responsible for the treatment of drinking water who faithfully seek compliance) can search the electronic Code of Federal Regulations and read that utilities serving a population less than 10,000 will not start monitoring their source water for cryptosporidium until April 1, 2010 (Rules and Regulations, 71 Fed. Reg. 753-786 (Jan. 5, 2006)).

A reader will also discover that cryptosporidium treatment requires filtration, as disinfection is non-effective and is resistant to traditional water utility treatments such as chlorine, hypochlorite, iodophors, formaldehyde, and pro-longed treatment of ammonia and saline of less than 18 hours (MSDS for cryptosporidium, Public Health Agency of Canada). The information provided meets the criteria for "in the public domain" as defined by the Department of Homeland Security, September 1, 2006:

> In response, in section 29.2(d), DHS has defined "in the public domain'' in part as information lawfully, properly and regularly disclosed generally or broadly to the public. This definition draws in part on section 214(c) of the CII Act (6 U.S.C. 133(c)), which stipulates that nothing in section 214 constrains the collection of critical infrastructure information including any information lawfully and properly disclosed generally or broadly to the public (Rules & Regulations, 71 Fed. Reg. 52,261-52,277 (Sept. 1, 2006)).

What is the lesson to be learned from the allegory of balancing the public right-to-know with the public health and safety? Water utility information is more restricted, as reported in the CRS Report for Congress, and are classified as FOIA exemption 3 prohibiting the disclosure of information and authorizing withholding under FOIA subsection (b) (3), but in the post-9/11 world information is still available, perhaps too much information, when motive, intent and knowledge come together (Stevens & Tatelman, Sept. 27, 2006).

A citizens' motive and intent differs from a terrorists' and yet in the post-9/11 world both groups, the citizen group and the terrorist group, can operate under the assumption a public agency acts in the agency's best interest and seeks compliance of the law, providing information upon request and following the requirements under the *Code of Federal Regulations*. The lesson is this: the FOIA laws become another terrorist's tool because the *motive* and *intent* of the terrorist is there, what they may lack is the *knowledge*.

This is where the balance tilts away from openness and transparency of government and tilts toward legislative remedies to protect the public. It does not suggest a permanent change in the shift in the balance, therefore the analogy of a scale, the counter-balance ever shifting, is appropriate. This is affirmed through the report *State Open Government Law and Practice in a Post-9/11 World* (Aug. 2007). As mentioned earlier: in Part 1, "Critical Infrastructures," forty-five states now have exemptions to FOIA regarding disclosure of information relating to building/architectural plans, vulnerability assessments, energy/public utilities information, mass transit and telecommunications systems (Dalglish, L.A., Cochran, L.A., Winegar, N., 2007). Currently, a total of twenty-two states enacted laws specifically exempting water systems from disclosure of information.

Conclusion

Publication of regulatory procedures and important information related to water utility systems still exists in the public domain. It is difficult to imagine water operators efficiently functioning without these "public domain" websites. As of 2007, twenty-two state exemption statutes specifically referenced water utility systems, water distribution lines, dams, or water related functions in their State exemption laws compared to ten states possessing similar restrictions in 2003. Water utility operators and security managers in states without FOIA legislative exemptions for water system information restrictions may begin to restrict information from public disclosure, as they press their State legislators for similar exemptions. As water security professionals become more knowledgeable regarding the use, limitations, restrictions, exemptions and exclusions in the Freedom of Information Act and the use of existing current state laws to protect critical infrastructure system design and information, one can expect more laws to seek protection for utilities from public exposure. One should also expect to see more state Attorney General opinions exempting water utilities from releasing information.

Based on the anecdotal evidence, it is expected the trend toward more secrecy and restrictions on water utility information will continue. As demonstrated by the Milwaukee incident, and the continuation of water contamination incidents, openness and sharing of information is not a guarantee of total public health and safety. As more public awareness of exemptions and security practices becomes common knowledge it is expected that further restrictions will be placed on water utility information once thought of as a community's right to know.

Reference Page

Herb Strenz, *A Rationale for Openness - all 6 versions,* 1 Comparative Media L. J. 92 (2003) Citing *Letter from James Madison to WT Barry*, Aug. 4, 1822 *in* The Complete Madison 337 (Saul Padover ed., 1953) *available at* http://www.juridicas.unam.mx/publica/rev/comlawj/cont/1/cts/cts5.htm.

B. B. Altera, *All the information the security of the nation permits: information law and the dissemination of air force environmental documents,* Air Force L. Rev.

American Water Works Association Applauds Enactment Of the Homeland Security Act of 2002, PR Newswire. Nov 25, 2002, *available at* General OneFile via Gale, http://find.galegroup.com/ips/start.do?prodId=IPS.

Richard N. L. Andrews, *Learning from history: U.S. environmental politics, policies, and the common good,* Environment 48.9, 28(17) (Nov 2006) *available at* General OneFile, Gale, http://find.galegroup.com/ips/start.do?prodId=IPS.

Assessment of inadequately filtered public drinking water - Washington, D.C., December 1993, Morbidity and Mortality Weekly Report 43 n36 p.661(3) (Sept 16, 1994), *available at* General OneFile via Gale, http://find.galegroup.com/ips/start.do?prodId=IPS.

Attorney General Open Records Letter Opinions Concerning Terrorism or Terrorist Activities, Dep't of State Health Services, Office of General Counsel. http://www.dshs.state.tx.us/comprep/ogc/agchart.DOC.

Phaedra S. Corso, Michael H. Kramer, Kathleen A. Blair, David G. Addiss, Jeffrey P. Davis, & Anne C. Haddix, *Cost of illness in the 1993 waterborne cryptosporidium outbreak, Milwaukee, Wisconsin,* Emerging Infectious Diseases 9.4, 426(6) (Apr. 2003), *available at* General OneFile, Gale, http://find.galegroup.com/ips/start.do?prodId=IPS.

Cost of illness in Milwaukee Cryptosporidium outbreak almost $100 million, Managed Care Weekly, May 26, 2003, p.13, *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

G. F. Craun, N. Nwachuku, R. L. Calderon, & M. F. Craun, *Outbreaks in drinking--water systems 1991-1998,* J. of Env't Health, 65, 1. p.16(8) (July-Aug. 2002), *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

R. Dahl, *Does secrecy equal security? Limiting access to environmental information,* Env't Health Perspectives 112, 2. p.A104(4) (Feb. 2004), *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

J. A. Davis, *Terrorism fears thwart journalists' reporting: is the public being well-served by the government's protection of information?* Nieman Reports 58, 2. p.18(2) (Summer 2004) *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

Denver Post, *Editorial: Secrecy Isn't Security*, Nov. 3, 2002.

H. Ellis, *Cranking up cryptocapitalism's wheel of fortune,* The Business J.-Milwaukee 12, n3 p.6A(2) (Oct 22, 1994) *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

Environmental, Homeland Security Laws Needed for Drinking Water Protection, A Scribe Law News Service p.NA (Nov 11, 2003), *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

National Primary Drinking Water Regulations: Long Term 2 Enhanced Surface Water Treatment Rule, Rules and Regulations, 71 Fed. Reg. 753-786 (Jan. 5, 2006).

Federal Register, 71 Fed. Reg. 52,261-52,277 (Sept. 1, 2006).

Gina Marie Stevens & Todd B. Tatelman, *CRS Report for Congress Protection of Security-Related Information*, Sept. 27, 2006.

HOMELAND SECURITY: New act must not sacrifice American way of life, Houston Chronicle, July 12, 2002.

Letter from James Madison to W.T. Barry (Aug 4, 1822), *in* The Writings of James Madison, (Gaillard Hunt ed. 1910).

F. W. Pontius & S. W Clark, Water Quality & Treatment, 5th ed., (AWWA, 1999).

Exec. Order 12958, *Classified National Security Information*, p 31109.

Public Health Agency of Canada, Office of Laboratory Security retrieved, Sept. 13, 2007, http://www.phac-aspc.gc.ca/msds-ftss/msds48e.html.

See EARLY WARNING MONITORING note 32, at 26, *supra* (citing Center for Disease Control estimates of up to 900,000 illnesses and possibly 900 deaths caused each year in the U.S. "as a result of waterborne microbial infections"); *see also* Kornfeld, *supra* note 2, at 467 ("Over the past decade a number of outbreaks, in the U.S., involving...Cryptosporidiosis (Crypto), have sickened at least 500,000 and killed hundreds."); *see also* Steve E. Hrudey & Richard Walker, Walkerton--*5 Years Later: Tragedy Could Have Been Prevented*, OPFLOW (Am. Water Works Assoc., Denver, Co.), June 2005, at 1 (discussing serious flaws within an Ontario municipal drinking water system that "aligned to permit a breakthrough of E. coli...causing seven deaths and more than 2,300 cases of waterborne disease").

S. D. Shermer, *The drinking water security and safety amendments of 2002: is America's drinking water infrastructure safer four years later?* UCLA J. of Env't L. & Policy 24, 2. p.355(103) (Winter 2006) *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

State Open Government and Practice in a Post-9/11 World, L. A. Dalglish, L.A. Cochran, N. Winegar eds, (Lawyers & Judges, 2007).

M. Ternus, *Water, water everywhere - but is it safe to drink?* Env't Nutrition, 18, n9. p.9(4) (Sept 1995), *available at* General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

Title 40: Protection of Environment, Part 141—National Primary Drinking Water Regulations, Subpart W—Enhanced Treatment for Cryptosporidium, Source: 71 Fed. Reg. 769 (Jan. 5, 2006, unless otherwise noted).

USA Patriot Act of 2001 § 1016, 42 U.S.C. § 5195c(e) (2006) (Critical infrastructures are "those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.") Other critical infrastructure includes, among other things, telecommunications systems, energy resources and distribution networks, banking and finance networks, transportation, food and wastewater systems, and emergency services.

Norfolk suffers from cryptosporidium contamination, Utility Week (Brief article) (June 22, 2007) p.NA, *available at* from General OneFile via Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

Welsh Water to pay cryptosporidiosis claims, Utility Week, NA (Dec 8, 2006), *available at* General OneFile Gale http://find.galegroup.com/ips/start.do?prodId=IPS.

2.2 State Laws Regarding Information About Critical Infrastructure

by James W. Conrad, Jr.[1]

Introduction

The six years since 9/11 have seen extraordinary change across virtually every field of substantive law. Legislatures and courts have been continuously busy rewriting preexisting law, from airline security to electronic surveillance to tort liability, as well as crafting law in entirely new fields such as chemical facility security and anti-ter-

1 Principal, Conrad Law & Policy Counsel, Washington, D.C.; J.D., George Washington University Law School; B.A., Haverford College.

rorism technology. Many of these changes have been extremely controversial, pitting fundamental constitutional rights like the privacy rights of air travelers and the due process rights of people like Jose Padilla against the specter of death and destruction on par with, and potentially worse than, that fateful day.

And yet, at the same time these legal battles have played out across front pages and TV screens, equal or more sweeping changes prompted by 9/11 have also proceeded almost unnoticed. A prime example is the legislation addressed by this paper—state enactments limiting the disclosure of information regarding the security of critical public or private infrastructure. A precise count of such laws would depend on how the category was defined, and even then would still be hampered by the difficulty of dealing with borderline cases. Easily 75% of the 50 states, however, have passed some sort of statute since 9/11 protecting information about security vulnerabilities, countermeasures or response plans associated with infrastructure. In its compilation of changes to state public information laws since that date,[2] the Reporters Committee for Freedom for the Press lists only eight states as not having some such law.

Even more remarkably, these statutes seem to be almost all *sui generis*—that is, they give every appearance of having been bottoms-up, spontaneous initiatives, rather than instances of a uniform or model statute that was developed by some interest group or institute and then systematically pushed through state legislatures. The strongest evidence for this theory of origin is the remarkable diversity of these laws. They differ on at least a dozen different parameters (e.g., breadth of coverage, standard for nondisclosure), and on many of those parameters they adopt up to a half-dozen different approaches.

This paper takes a largely descriptive approach, listing the most important parameters and illustrating the diversity of approaches taken by different laws. Where I am aware that a court or other decision-maker has adjudicated a statute, I discuss that precedent. (However, it seems from both the Reporters Committee document and my own experience that the application of these statutes has very rarely been evaluated by tribunals.) At times, I offer editorial opinions regarding the wisdom or danger of particular approaches. While these statutes may not trample directly on any constitutional protections, they do impinge on the public's right to know, which has achieved a sort of quasi-constitutional status.

To establish a standard of comparison, the paper begins by describing how federal law governs the disclosure of information regarding the security of infrastructure. The paper then identifies a set of significant parameters and discusses how the laws identified in the Reporters Committee document vary across those parameters. At the end, I offer some concluding thoughts. In a nutshell, my conclusion is that the relatively low level of public controversy associated with these statutes is probably appropriate—it does not appear that they have, in fact, inspired a qualitatively new level of state government secrecy.

As the reader reviews the paper, he or she should bear in mind the basic ways that security-related information could become public, i.e., through disclosure by:

- The relevant sovereign;
- A subordinate governmental instrumentality; or
- A private entity;

either:

- Voluntarily;

2 Reporters Comm. For Freedom of the Press, State Open Government Law and Practice in a Post-9/11 World – Changes in State Public Information Laws in the United States Since the War on Terrorism (Jeffrey Addicott, Lucy Dalglish, Loren Cochran, & Nathan Winegar eds., Lawyers & Judges 2007). This paper generally limits itself to the authorities discussed in that compilation. While I have conducted some additional research for the paper, I have not attempted to assess the compilation's completeness or to independently replicate it.

- In response to a request under the Freedom of Information Act (FOIA) (in the case of the federal government) or comparable open records laws (in the case of state or local governments); or
- Pursuant to judicial process.

I. Federal Law Applicable to Information about the Security of Critical Infrastructure

There are potentially multiple ways for the federal government to avoid having to disclose information about the security of infrastructure, including one—classification on national security grounds—that only the federal government can exercise.[3] Aside from classification, however, in the great majority of cases, two authorities are likely to be the basis on which the federal government might refuse to disclose infrastructure security information, or seek to prevent others from doing so. These two authorities also serve as a useful yardstick by which to judge state enactments directed toward the same end.

A. Sensitive Security Information (SSI)

Both the Department of Transportation (DOT) and the Transportation Security Administration (TSA, part of the Department of Homeland Security (DHS)) have statutory authority to issue regulations, "[n]otwithstanding [FOIA]," that "prohibit[] disclosure of information obtained or developed in ensuring security" (DOT) or "in carrying out security" (TSA) under regulatory programs they administer, if the relevant agency finds that "disclosing the information would . . . be detrimental to transportation safety" (DOT) or "transportation security" (TSA).[4] The two agencies have jointly issued rules implementing this authority.[5] These rules largely address aviation security (regulated by TSA) and maritime security (regulated by the Coast Guard), but a few of the rules are written so generally that they apply in any transportation setting.

The rules identify over a dozen 'categorical inclusions;' i.e., if information falls into one of these categories, it is automatically SSI. These include "vulnerability assessments," "threat information," "security programs and contingency plans," "security inspection or investigative information," "security measures," and "critical aviation or maritime infrastructure asset information."[6] The two agencies can also conclude that other information meets the statutory definition.[7]

The SSI rules allow DOT and TSA to make SSI available to the relevant players in the aviation and maritime security context—i.e., "covered persons"—who by rule or agency decision have a "need to know" that SSI.[8] Those persons are in turn authorized to give SSI to others meeting the same description. Like the procedures for classified information, the SSI rules are legally binding on private persons who possess SSI, including those who generate the information in the first place. Violations of the SSI rules by governmental or private actors are "grounds for a civil penalty and other enforcement or corrective action" by the relevant agency.[9]

The SSI rules (and the statutory authority underlying them) thus prevent government personnel from voluntarily disclosing SSI outside of regulatory channels, and provide TSA and DOT with a basis for denying FOIA requests for such information. Because the federal government has concluded that the SSI rules preempt state law, they have the same effect on state and local governments.[10] And

3 This general topic is the subject of my article, James Conrad, *Protecting Private Security-Related Information from Disclosure by Government Agencies*, 57 Admin. L. Rev. 715 (2005).

4 49 U.S.C. §§ 114(s)(1), 40119(b)(1).

5 49 C.F.R. Parts 15 (TSA) and 1520 (DOT).

6 *Id.* §§ 15.5(b), 1520.5(b).

7 *Id.* §§ 15.5(b)(16), 1520.5(b)(16).

8 *Id.* §§ 15.7, 15.11, 1520.7, 1520.11.

9 *Id.* §§ 15.17, 1520.17.

10 *See e.g.*, 68 Fed. Reg. 60469 (Oct. 22, 2003) (TSA and Coast Guard agree that SSI rules preempt conflicting state disclosure laws).

for the reasons just discussed, they prevent private persons from disclosing SSI without approval.

While the statutes and rules do not speak directly to judicial process, DOT and TSA have taken the position that the rules apply to litigants just like any other persons, and TSA has invoked SSI authorities as the basis for refusing to provide SSI to persons in litigation with the government,[11] and for intervening to prevent others from releasing SSI in litigation.[12]

The aggressiveness with which the federal government has asserted its SSI authorities has led to repeated Congressional criticism, culminating last fall in appropriations legislation that provides a means for litigants to obtain SSI under standards somewhat like those that apply to attorney work product.[13]

B. Protected Critical Infrastructure Information

Part of the Homeland Security Act enacted in 2002, the Critical Infrastructure Information Act (CIIA)[14] attempts to encourage unregulated critical infrastructure sectors to voluntarily share security-related information with DHS by providing that information with an unprecedented type of protection. Under this law and rules issued under it by DHS, "critical infrastructure information"[15] that is "voluntarily"[16] submitted to the "Protected Critical Infrastructure Information (PCII) Program Office" at DHS is exempt from disclosure under FOIA.[17] Criminal penalties are established for federal employees who "knowingly" release the information.[18] In addition, among other things:

- The information is also exempt from disclosure under any state or local 'FOIA' or "sunshine" laws;[19] and
- If submitted in "good faith," the submitted information cannot itself be used "directly" in any governmental civil enforcement action, or in any private civil lawsuit, in federal or state court.[20]

DHS can share the information within the federal government and with state and local governments—and contractors working for them—but all of these entities can only use it for purposes of:

- Infrastructure protection; or
- Investigating or prosecuting crimes.[21]

The PCII program does not allow would-be submitters to "launder" or otherwise conceal information currently required to be made public. Regulated entities must continue to report to the federal government any information that they are required to report under any other law, and federal, state and local agencies continue to have all their existing powers under other laws to obtain records and other information that regulated entities are required to make available to them.[22]

Unlike the SSI regime, the PCII program is not self-implementing—it applies only if information is submitted to DHS and DHS "validates" it as fitting the definition of PCII.[23] Also unlike the SSI regime, the PCII program imposes no obligations on nonfederal persons generating (or otherwise in possession of) PCII—they can freely release it, although it is then no longer protected.

11 See e.g., *Gilmore v. Gonzales*, 435 F.3d 1125, 1133 n.8 (9th Cir. 2006).
12 See, e.g., *In re Sept. 11 Litigation*, 431 F. Supp. 2d 405, 407-411 (S.D.N.Y. 2006).
13 See Pub. L. No. 109-295, § 525(d).
14 6 U.S.C. §§ 131-34.
15 "Critical infrastructure information" basically means information not customarily in the public domain regarding threats, vulnerabilities and related problems or solutions affecting critical infrastructure or the physical or cyber resources that support it. *Id.* § 131(3).
16 "Voluntarily" means not in response to DHS's exercise of its power "to compel access to or submission of the information." *Id.* § 131(7)(A).
17 *Id.* § 133(a)(1)(A).
18 *Id.* § 133(f).
19 *Id.* § 133(a)(1)(E)(i).
20 *Id.* § 133(a)(1)(C).
21 *Id.* § 133(a)(1)(E)(iii).
22 *Id.* §§ 133(c), (d); 6 C.F.R. § 29.8.
23 6 C.F.R. §§ 29.5, 29.6.

I am unaware of a case in which litigants have attempted to obtain PCII from the federal government or a private entity, but in its PCII rules, DHS has taken the position that PCII is not discoverable or admissible in litigation other than criminal prosecutions.[24]

Finally, on a related point, the Homeland Security Act also empowered the Secretary of Homeland Security to issue exemptions from the Federal Advisory Committee Act, and he has done so for meetings of a new entity called the Critical Infrastructure Partnership Advisory Committee, facilitating the exchange of critical infrastructure information between the federal government and private infrastructure owners and operators.[25]

The PCII program has also had its critics in the right-to-know community[26] and Congress, but legislation to commission a critical GAO study of the program was recently dropped from the Senate version of pending FOIA amendment legislation.[27]

II. State Statutes

As noted earlier, the multitude of state laws regarding information about the security of critical infrastructure differs across about a dozen parameters:

A. Whose information is covered?

Under most of the statutes, it does not matter who generated the information in question. Many are more limited, however. For example, the Arizona statute addresses risk assessments performed "*by or on behalf of a federal agency* regarding critical energy, water or telecommunications infrastructure."[28] The California statute covers only documents prepared "*by or for a state or local agency*."[29] Such a narrow focus seems unwise, or at least likely to require later amendment to add assessments conducted by others or voluntarily. The Arizona law could also be superfluous, at least in the case of information that constitutes SSI or PCII.[30]

B. Breadth of coverage.

The fundamental premise of the Reporters Committee compilation is that the statutes it has compiled in the "Critical Infrastructure" category address security-related information about critical infrastructure. Many do cover the category generally. Others are limited to specific sectors or activities. For example, the Arkansas law covered only computer or telecommunications infrastructure and public water systems.[31]

Some statutes, however, sweep quite a bit more broadly. Perhaps the most dramatically sweeping coverage is the Alabama statute, which covers "records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures, including without limitation information concerning critical infrastructure. . . the public disclosure of which could reasonably be expected to be detrimental to the public safety or welfare, and records the disclosure of which would otherwise be detrimental to the best interests of the public."[32] An exemption that covers any information about the "security . . . of persons" pretty well exempts all security-related information—which may be appropriate, so long as the

24 *Id.* §§ 29.8(f)(1)(A), (i); 71 Fed. Reg. 52264-65.

25 *See* 6 U.S.C. § 871; 71 Fed. Reg. 14930 (Mar. 24, 2006).

26 *See, e.g.*, Rena Steinzor, *Democracies Die Behind Closed Doors: The Homeland Security Act and Corporate Accountability*, 12 Kansas J. L. & Pub. Pol'y 641, 643 (2003).

27 The GAO study would have been commissioned by Section 12 of the OPEN Government Act of 2007, S. 849 and H.R. 1326, as introduced on March 13 and March 5, 2007, respectively. However, that section is absent in S. 849 as passed by the Senate on August 3, 2007.

28 Ariz. Rev. Stat.§ 39-126 (emphasis added).

29 Cal. Gov't Code § 6254(aa) (emphasis added).

30 *See* text accompanying notes 10 and 19, *supra*.

31 Ark. Code Ann. § 25-19-105. According to the compilation, the law sunset in July 2007.

32 Ala. Code § 36-12-40.

standard for nondisclosure is not too low (which I think is a problem here; see Part II.E below)—but it is important that such legislation be fairly advertised for what it is, which is a lot more than just critical infrastructure.

The Alabama statute and many others are also notable in that their coverage turns on risks not just to "security," but also "safety."[33] Again, this may be appropriate if the standard for nondisclosure is not too law, but the scope of coverage is enormous, which understandably can raise concerns about the potential for excessive secrecy.

C. Is the statute limited to terrorism concerns?

Since 9/11 was the paradigmatic terrorist attack against the United States, it is only natural that about half of the statutes covered in the Reporters Committee compilation use words like "terrorist attack"[34] or "act of terrorism"[35] in defining their scope. Others use more oblique words like "security,"[36] which at least is limited to the concept of illegal entry or attack. But several statutes refer simply (or additionally) to "criminal acts."[37] This seems unnecessarily broad, and could result in a wide range of information being kept secret, potentially more to avoid governmental embarrassment than to prevent terrorist attacks. For example, the vulnerability of a state health insurance program to fraud is likely to be a subject of public interest and not of great relevance to terrorists.

D. Types of documents covered

Some of the statutes compiled by the Reporters Committee refer to a laundry list of common security-related documents like vulnerability assessments and security plans, either preceding or following a catch-all descriptive clause.[38] This seems sensible, so long as the standard for nondisclosure (see Part II.E below) is not too low—the types of documents that can pose security risks if disclosed are so varied that any specific enumeration is bound to be under inclusive. Yet a number of statutes are limited to such enumerations,[39] and some of them are not very long; for example, the Wisconsin statute protects only "plan or specifications for state buildings."[40]

Several of the statutes employ various limiting adjectives like "specific and unique" [41] or "specialized details"[42] to limit the kinds of documents protected. While the precise meaning of such words in a given case may be obscure, at least they give some indication of legislative intent to limit withholding. This kind of limitation seems to have been effective in the case of one of the Texas statutes. The Texas Attorney General rejected a municipal water authority's attempt to withhold a report revealing management problems associated with its software system, holding that the authority had "not identified which portions of the quality control audit consist of *technical details of particular vulnerabilities of critical infrastructure to an act of terrorism*."[43]

E. Standard for nondisclosure

The statutes compiled by the Reporters Committee vary widely in how demanding their standards for nondisclosure are. Some statutes include a number of limiting adjectives and adverbs that would seem to give disclosure proponents some amount

33 *Id*; *see also* Conn. Gen. Stat. § 1-210(a)(19); Mass. Gen. Laws ch. 4, § 7(n) (among others).
34 *See, e.g.*, Ind. Code § 5-14-3-4(b)(19).
35 *See, e.g.*, Fla. Stat. Ann. § 395.1056(1)(a).
36 *See, e.g.*, Or. Rev. Stat. § 192.502(32).
37 *E.g.*, Cal. Gov't Code § 6254(aa), Ga. Code Ann. § 50-18-72(a)(15)(A); Neb. Rev. Stat. § 84-712.05(8).
38 *E.g.*, Ala. Code § 36-12-40; Ga. Code Ann. § 50-18-72(a)(15)(A); Idaho Code § 9-340B (4)(b); Utah Code Ann. § 63-2-106.
39 *E.g.*, W. Va. Code § 29B-1-5(a).
40 Wis. Stat. Ann. § 19.36(9).
41 *See* Del. Code Ann. tit. 29, § 10002(g)(16)a.5.A.
42 Colo. Rev. Stat. Ann. § 24-72-204(2)(a)(VIII).
43 Tex. Atty. Gen. Op. OR2007-10996, 2007 WL 2462472 (Aug. 23, 2007) (italicized words are from Tex. Gov't Code Ann. § 418.181).

of comfort about the reality or degree of harm that they can justify withholding. For example, the Alaska law only allows withholding of records where disclosure "could *reasonably* be expected to endanger the life or physical safety of an individual or to present a *real and substantial* risk to the public health and welfare."[44] The Illinois statute is even more demanding, requiring disclosure to "constitute a clear and present danger to the health or safety *of the community*"[45]—rather than "an individual" or "any person"—which seems appropriate given the types of mass casualty attacks that homeland security law generally is designed to prevent.

At the other extreme, as noted in above, the Alabama statute allows the state to withhold "records . . . the public disclosure of which could reasonably be expected to be detrimental to the public safety or welfare [or] *would otherwise be detrimental to the best interests of the public*."[46] This standard seems unjustifiably low, as by definition the italicized language would only apply to records that cannot reasonably be expected to jeopardize public safety or welfare. What other risks are being averted here? The standard created by the italicized language certainly evinces a paternalistic type of discretion of a sort that legislatures generally have not dared to give bureaucrats in recent decades.

On the other hand, concerns about undue secrecy arising from a very general threshold for withholding should be mitigated to some extent by a recognition that the same generality that could support over withholding can also be consistent with a strong bias for release. For example, the Connecticut statute on its face sets up a relatively low threshold: whether "there are reasonable grounds to believe that disclosure may result in a safety risk, including the risk of harm to any person….."[47] A town opposed the release of GIS (geographical information systems) data about it (aerial photography, primarily) with testimony by the chief of police that the photographs could aid professional criminals by revealing security measures that homeowners had put in place.[48] While such a statement could conceivably meet the statutory standard, the state supreme court unanimously concluded "[s]uch generalized claims of a possible safety risk…did not…establish a nexus between [the police chief's] opinion and the conclusion that the release of the data would pose a safety risk."[49]

Beyond risks of harm, some state statutes also track federal law in allowing withholding where disclosure:

- "could reasonably be expected to interfere with implementation or enforcement of the security plan, program or procedures"[50] (somewhat comparable to the "law enforcement sensitive" exemption to FOIA's disclosure mandate[51]); or
- "would disclose confidential guidelines for investigations or enforcement [that] could reasonably be expected to risk circumvention of the law"[52] (effectively the same as the "risk of circumvention" or "high 2" interpretation of the FOIA exemption regarding "internal personnel rules and practices of an agency").[53]

44 Alaska Stat. § 40.25.120(a)(10)(C) (emphasis added). The first half of that clause is taken verbatim from the law enforcement sensitive exemption of FOIA, 5 U.S.C. § 552(b)(7)(F).

45 5 Ill. Comp. Stat. Ann. § 140/7(1)(ll) (emphasis added).

46 Ala. Code § 36-12-40 (emphasis added).

47 Conn. Gen. Stat. Ann. § 1-210(b)(19).

48 Director, Dep't of Info. Tech. v. FOI Comm'n; 274 Conn. 179, 874 A.2d 785 (2005).

49 274 Conn. at 193, 874 A.2d at 794.

50 Alaska Stat. § 40.25.120(a)(10)(A).

51 5 U.S.C. § 552(b)(7)(A).

52 Alaska Stat. § 40.25.120(a)(10)(B).

53 5 U.S.C. § 552(b)(2); *see Conrad*, *supra* note 3, 57 Admin. L. Rev. at 733-34.

F. Does a central state agency make final decisions about withholding information?

I noted at the outset that there appear to be very few judicial or administrative decisions interpreting the statutes compiled by the Reporters Committee, which is initially surprising given the number of such statutes and the degree of controversy, at least at the federal level, associated with the government withholding of information on security grounds. The chief exception to this generalization is Texas, where the state Attorney General issues informal opinions roughly twice a month interpreting three related statutes concerning information about emergency response providers, risk or vulnerability assessments, and critical infrastructure.[54] Otherwise, it appears that the only state high court to address one of these statutes is the Connecticut Supreme Court.[55] It may not be accidental that this activity has occurred in two states whose freedom of information law empowers a central state agency to make final administrative decisions regarding withholding of information. In Connecticut, a person whose request for information has been denied may appeal that denial to the state Freedom of Information Commission,[56] and in such an appeal the burden of persuasion is on the denying agency to show that its decision to withhold was correct.[57] In Texas, the state or local agency seeking withhold information must ask the state Attorney General to decide whether that decision is correct.[58] It seems entirely plausible that a state agency tasked with interpreting a statute with a bias toward disclosure is likely to reach decisions to release information much more readily than an agency that has other missions, missions that such agency may feel are undercut or frustrated by the obligation to release information.

G. Is nondisclosure discretionary or mandatory?

One thing that private sources of security-related information have made abundantly clear is that they are very unlikely to share such information with governmental entities if there is any uncertainty about whether it will be protected.[59] That is why such sources prefer laws and rules that are written in terms like "shall not be disclosed" rather than ambiguous phrases like "is exempt from disclosure" (which could mean exempt from mandatory disclosure, but still disclosable at the government's discretion), or worse yet language that expressly makes disclosure discretionary.[60] The Virginia and District of Columbia statutes suffer from this flaw, and probably have not promoted much submission to those governments.[61]

H. Does a private submitter of information get notice of a request for that information?

Under FOIA, an executive order ensures that, whenever an agency receives a request for private information that the submitter has claimed to be confidential business information, the agency must notify the submitter and give it an opportunity to object to disclosure and explain why.[62] Some state critical infrastructure statutes have expressly included a similar notice requirement,[63] which should encourage voluntary submittals by private entities. It also should aid states in making

54 Tex. Gov't Code Ann. §§ 418.176, .177 & .181.
55 *See* note 48, *supra*.
56 Conn. Gen. Stat. Ann. § 1-206(b)(1).
57 Director, Dep't of Info. Tech, *supra* note 48; 274 Conn. at 187, 874 A.2d at 791.
58 Tex. Gov't Code Ann. § 552.301(a).
59 Homeland Security Advisory Council Private Sector Information Sharing Task Force, Homeland Security Information Sharing Between the Government and the Private Sector at15-16, 24-27 (Aug. 2005).
60 *See Conrad, supra* note 3, 57 Admin. L. Rev. at 723 n. 18 and accompanying text.
61 *See* Va. Code Ann. § 2.2-3705.2 ("The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law."); DC Code Ann. § 2-534(a) ("The following matters may be exempt from disclosure…..").
62 E.O. 12600, 52 Fed. Reg. 23781 (June 25, 1987).
63 Ala. Code § 36-12-40.

disclosure decisions, particularly if submitters are not required to substantiate requests for protection at the time of submittal.

I. Does a private source of the information need to request coverage?

In Part II.F, I discussed statutes that require a state or local agency seeking to withhold information to obtain the approval, initially or on appeal, of another state agency. A different issue arises in the case where the information in question was submitted by a private entity: is the private entity's information automatically protected, or does the entity have to invoke the law's protection? As with the PCII program (or the FOIA exclusion regarding confidential business information[64]), the Virginia statute appears to apply only to privately submitted information where the submitter invokes its protections.[65] Even then, however, the Virginia statute says the information "may" be withheld from disclosure,[66] which does not inspire confidence.

J. Does the law allow some degree of protected information sharing?

As noted in the discussion of the federal PCII and SSI regimes, enhancing security generally requires the relevant federal, state, local and private actors to be able to share sensitive information with each other without thereby being required to release it to anyone. In this spirit, the Maine statute specifically provides that information otherwise prohibited from disclosure under it may be shared with "municipal officials or board members under conditions that protect the information from further disclosure."[67] The Florida statute is similar.[68]

The Washington statute specifically exempts from disclosure "records not subject to disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism."[69] To the extent such records are covered by the PCII program or constitute SSI (which respectively override state and local open records laws expressly and impliedly), such an exemption would be unnecessary. But it is a helpful contribution to the cause of intergovernmental information sharing, something that (i) is necessary for effective protection and (ii) does not occur adequately, in the view of most state and local officials.

The Tennessee statute presents a good example of bad information sharing language, preserving the right of access to protected information "by other governmental agencies performing official functions" (so far so good), but then allowing "any governmental agency [to] allow[] public access to the records during the course of an official function."[70] Perhaps the fire marshal should be able to inspect security plans to see if physical security measures might obstruct egress from the facility in the event of a fire, but he or she should not be given blanket authority to make such information public in the process.

K. Is there a judicial escape clause?

The Florida statute is somewhat unusual in expressly providing that "a court of competent jurisdiction" may order disclosure of a protected document "upon a showing of good cause." While this sort of judicial escape clause is probably a good idea (and might well be invented by a court in any event), the statute could be clearer (i) about what would constitute good cause (e.g., when the public interest in disclosure outweighs the risks to the public caused thereby), and (ii) that disclosure could be under terms that would limit further disclosure.

64 5 U.S.C. § 552(b)(4).
65 Va. Code Ann. § 2.2-3705.2 (4).
66 *Id.*
67 Me. Rev. Stat. Ann. tit. 1, § 402.3.L.
68 Fla. Stat. Ann. § 119.071(3)(c).
69 Wash. Rev. Code § 42.56.420(1)(b).
70 Tenn. Code Ann. § 10-7-504(21)(D).

L. Does the law preserve existing requirements regarding public availability of information?

As noted above, the federal PCII rules are clear that they do not allow facilities to get disclosure protection for information that other law requires to be reported or made available to federal agencies. Oddly, given the degree of attention this issue has attracted whenever Congress has debated the issue, most of the statutes in the Reporters Committee compilation do not address it. The Delaware and Ohio laws are exceptions.[71]

M. Does the statute create an exemption from open meetings laws?

A few of the statutes in the Reporters Committee compilation appear to be exemptions from open meetings laws, not open records laws.[72]

III. Concluding Thoughts

Virtually all of the state statutes contained in the Reporters Committee compilation were enacted in 2002 or, to a diminishing extent, the next two years, and so almost all have now been in place for three to five years. Over this period, it appears that very rarely has a frustrated requestor sought review of a state's denial of that person's request for information. Rather, it seems that private citizens, journalists and others have not needed the sort of information that these laws protect in order to do their jobs or go about their lives. This has happened, moreover, even though most of these laws do not contain clauses expressly assuring the continued availability of information previously required to be reported or made available to the government. In sum, the harms that might have been predicted to follow from these statutes appear not to have materialized.

Moreover, the laws do serve a valuable purpose. Since 9/11, public and private entities have embarked on an ambitious program of assessing their vulnerabilities to terrorist attack and developing security and response plans to prevent or respond to such an attack. While some of these locations may not be likely to top any terrorists' target lists, many others could experience (or cause) substantial adverse consequences if attacked. Presumably most Americans would agree that, at some level of specificity and at some threshold for nondisclosure, this information should be protected from public release.

Most states have already enacted such legislation, though it has sunset in several cases. Other states may yet address this issue, and the sunset states may wish to enact new legislation. Finally, some states might want reconsider or optimize the legislation they have already enacted. Based on my review of the statutes contained in the Reporters Committee compilation, I would venture that a model law would:

- Protect infrastructure security information regardless of whether it was prepared by federal, state, local or private entities.
- Protect information about any type of critical infrastructure, rather than specific categories such as water treatment systems.
- Protect specific information the public release of which would be reasonably likely to pose real risks to the community from acts of terrorism, not just criminal activity.
- Provide an administrative appeal to some central state agency of decisions by other state or local agencies to withhold information under the law.
- Provide that withholding of information protected by the statute is mandatory and that violations are subject to sanctions.

71 *See* Del. Code Ann. tit. 29, § 10002(g)(16)a 2; Ohio Rev. Code Ann. § 3750.22(B)(2) (not exempting private owner/operators from providing information to the public when required by any other federal or state law).

72 *E.g.*, 35 Pa. Cons. Stat. § 2140.202(c).

- Provide prior notice to private entities of an initial decision to disclose information they have submitted.

- Not require private submitters to request protection of information they submit.

- Allow state and local agencies in possession of protected information to share it with other federal, state, local and private entities where warranted to enhance security or preparedness, with provisions for continued protection, without thereby waiving the protections of the law.

- Address the standards and conditions under which courts may allow disclosure of the information to others.

- Provide that information currently required to be reported or made available to a government agency remain subject to such requirements.

- Not contain a sunset clause.

2.3 Exempting Critical Infrastructure Information: More Harm Than Good

by Harry Hammitt

After the terrorist attacks on September 11, 2001, government scrambled to reduce potential vulnerabilities to protect against such future attacks. Responding more from fear than from measured deliberation on how best to solve these problems, the Bush administration trotted out a litany of shop-worn programs and expanded powers that, cobbled together in a matter of weeks, was passed by Congress as the Patriot Act. One aspect of the debate that began to receive attention from both executive agencies and Congress was the extent to which publicly available information might be used by terrorists to plan and execute future attacks. Many agencies, most notably the Nuclear Regulatory Commission, began to scrub their websites of information that only weeks before had been considered useful and beneficial to the general public and the constituencies served by various agencies. In no time at all, public information, which had long been considered a vital part of our democratic society, became instead a suspect commodity to be withheld from all those who did not have a crucial need to know. While a good deal of the information removed from websites immediately after September 11 has since been restored, government information policy remains stuck in a post-9/11 world in which the right to know has been rolled back and the need to know is the default position.

Perhaps one of the most wrong-headed initiatives from an information policy perspective has been the Critical Infrastructure Information Act, part of the Homeland Security Act creating the Department of Homeland Security, which provided a blanket exemption from disclosure under the Freedom of Information Act for critical infrastructure information provided to the Department. As with much of the flurry of legislation passed in the immediate wake of September 11, the creation of the Department of Homeland Security seemed like a good way of effectively rearranging government's ability to protect against terrorist threats and to respond to them if one were to occur again. But, as is often the case with hastily crafted legislation, many provisions were poorly thought out and were subject to little or no congressional debate before passage. The Critical Infrastructure Information Act was one such instance.

The debate over critical infrastructure information predates the terrorist attacks of September 11. In 1999, Congress held several hearings and legislation was introduced after the EPA announced that it intended, as part of its public disclosure obligations under amendments to the Clean Air Act, to post on the Internet what are known as worst-case scenario reports—assessments of potential environmental damage that could occur if a catastrophic event took place at a manufactur-

ing facility that stored chemicals or other hazardous materials. Such reports were required to help facilitate emergency response planning and to allow people to assess the risks such facilities posed for the community. After the EPA announced that it would make these reports available on the Internet, the chemical manufacturing industry protested and was able to convince the FBI that such widespread dissemination would allow terrorists to assess the vulnerabilities of such plants and maximize the potential damage from an attack. As a result of the hearings, Congress commissioned a two-year study of the problem. However, there is no apparent evidence that such a study ever actually took place and worst-case scenarios have in recent years been available in hard copy at various locations in the pertinent communities, but are not available to a wider audience and are not available at all in electronic form.

The worst-case scenarios controversy dovetailed with a related concern then being brought up in Congress—the possibility that computers would fail to properly recognize the date change when the calendar moved from 1999 to 2000, potentially causing massive equipment failures. An important part of assessing the potential for such trouble was to encourage the private sector to share its concerns about vulnerabilities with the government. To encourage such information-sharing, Congress passed Y2K legislation that prohibited disclosure of any such voluntarily-submitted information under FOIA and also excused the private sector from any potential liability if their products did fail as a result of the date change.

The issue of protecting critical infrastructure information more generally was still being discussed when the Bush administration took office and some form of legislation might well have been passed in the next year or two. But the attacks of September 11, 2001 tied the issue more closely to terrorism. Instead of being an issue about protecting confidential business information, it was now rolled into the push to protect the nation from future terrorist attacks. As part of the Homeland Security Act of 2002, the House of Representatives passed a provision allowing the Department of Homeland Security to protect voluntarily-submitted critical infrastructure information. In the Senate, public interest groups helped craft a provision that, while allowing such voluntary submissions, would allow outside challenges, based on the D.C. Circuit's decision in *Critical Mass v. NRC*,[73] as to whether or not specific submissions did indeed qualify as critical infrastructure information. The amendment, offered by Sen. Robert Bennett (R-UT), Sen. Patrick Leahy (D-VT), and Sen. Carl Levin (D-MI) was adopted by the Senate but was dropped in conference, leaving the House provision as the final version.

In its final version, the Critical Infrastructure Information Act[74] allows the Department of Homeland Security to receive voluntarily submitted information relating to critical infrastructure from the public, owners and operators of critical infrastructure, and state and local governmental entities in confidence while limiting public disclosure of that sensitive information under both the FOIA and any other federal or state laws. These provisions qualify as an Exemption 3[75] statute under FOIA, a catch-all exemption allowing other statutory provisions providing for non-disclosure of information to be applied through FOIA. It is important to note that the initial policy debate over the provision as it worked its way through Congress was whether an Exemption 3 statute, which allows agencies to withhold records whose disclosure is prohibited or restricted by a provision in another statute as long as that statute either provides no discretion on the part of the agency or identifies specific types of information to be withheld, was required or whether other existing exemptions, particularly Exemption

73 *Critical Mass Energy Project v. NRC*, 975 F.2d 871 (D.C. Cir. 1992) [hereinafter *Critical Mass*].

74 Codified as Homeland Security Act of 2002, Pub. L. 108-275, tit. II, subtitle B, § 211, 116, Stat. 2135, 2150 (Nov. 25, 2002) (6 U.S.C. § 131-134).

75 5 U.S.C. § 552(b)(3)

2[76]—which protects information the disclosure of which could result in circumvention of law or regulation—, Exemption 4[77]—which protects confidential business information submitted to government agencies—, or Exemption 5[78]—which protects information that is privileged in litigation—were adequate to provide protection. While neither proponents nor opponents of the provision were able to show to a certainty that existing exemptions would or would not protect the bulk of critical infrastructure information, it was clear that a specific tailored Exemption 3 provision would provide blanket protection—the preferred position of government and industry—while the combination of existing exemptions might allow a court to reject protection for certain types of information that did not seem to meet the threshold of being critical infrastructure information.

Critics of the provision were even willing to accept the analytical basis for determining what constituted a voluntary submission contained in the D.C. Circuit's *Critical Mass* decision. Under the *Critical Mass* test, information voluntarily submitted to government which is of a type that is not customarily disclosed by the submitter is presumed to be confidential. But information that is required to be submitted or whose submission the agency has statutory authority to require, will be analyzed under the earlier *National Parks* test,[79] which requires the agency or the submitter to show that disclosure will likely cause substantial competitive harm. From the beginning of the debate over critical infrastructure information, the position of industry had been that it was unwilling to trust its critical infrastructure information to renegade judges.

Senator Leahy has continued to push for changes in the Critical Infrastructure Information Act that would restore the balancing test that he, Bennett and Levin sponsored in the Senate. He introduced the Restore FOIA Act in March 2003 to amend section 204 of the Homeland Security Act. In introducing the legislation, he observed that the bill "would correct the problems in the HSA in several ways. First, it limits the FOIA exemption to relevant 'records' submitted by the private sector, such that only those that actually pertain to critical infrastructure safety are protected. 'Records' is the standard category referred to in FOIA. This corrects the effective free pass given to industry by the HSA for any information it labels 'critical infrastructure.' Second, unlike the HSA, the Restore FOIA bill allows for government oversight, including the ability to use and share the records within and between agencies. It does not limit the use of such information by the government, except to prohibit public disclosure where such information is appropriately exempted under FOIA." Another provision, Leahy explained, "allows local authorities to apply their own sunshine laws. The Restore FOIA bill does not preempt any state or local disclosure laws for information obtained outside the Department of Homeland Security. Likewise, it does not restrict the use of such information by state agencies."[80] Leahy also offered an implicit criticism of the way in which the original bill had been handled by the congressional Republicans. He noted that the Restore FOIA Act was "identical to language I negotiated with Senators Levin and Bennett last summer when the HSA was debated by the Governmental Affairs Committee. Senator Bennett stated in the Committee's July 25, 2003 mark up that the administration had endorsed the compromise. He also said that industry groups had reported to him that the compromise language would make it possible for them to share information with the government without fear of the information being released to competitors or to other agencies that might accidentally reveal it. The Governmental Affairs Committee reported out the compromise language that day. Unfortunately, much more restrictive House language was eventually signed into law."[81]

76 5 U.S.C. § 552(b)(2)
77 5 U.S.C. § 552(b)(4)
78 5 U.S.C. § 552(b)(5)
79 *National Parks & Conservation Association v. Morton*, 498 F.2d 785 (D.C. Cir. 1974).
80 Cong. Record, Mar. 12, 2003, p. S3632.
81 *Id.*

Leahy's bill did not move during that session of Congress. However, he reintroduced the bill in the next session of Congress on March 15, 2005.[82] Further, Leahy included auditing requirements for the critical infrastructure information provisions in the OPEN Government Act of 2007 (S.R. 849), which were also included in the House version (H.R. 1309). These provisions would require the Government Accountability Office to report annually for three consecutive years on the "number of persons in the private sector, and the number of State and local agencies, that voluntarily furnished records to the Department [of Homeland Security] under this section, the number of requests for access to records granted or denied under this section. . .[and] an examination of whether the nondisclosure of such information had led to the increased protection of critical infrastructure."[83] Resolving a hold placed on the OPEN Government Act by Sen. Jon Kyl (R-AZ), acting on behalf of the Justice Department, Leahy agreed to some changes, including dropping the reporting requirements, which had become the target of a separate last-minute hold by none other than Sen. Bennett. The amended bill has since been passed by the Senate. Regardless of the lack of success of Leahy's attempt to revise the critical infrastructure information provisions of the Homeland Security Act, his continued commitment to such changes reflects a strong attitude in the FOIA community that the current provisions are inappropriate.

The Department of Homeland Security issued proposed regulations concerning the voluntary submission of critical infrastructure information in 2003,[84] published an interim rule in 2004[85] and issued a final rule in August 2006.[86] The original proposal suggested that critical infrastructure information could be submitted to other agencies and could then be passed along to Homeland Security. The statutory language appears to contemplate that such submissions can only be made to the Department of Homeland Security and public interest groups were concerned that allowing other agencies to collect the submissions expanded the provision's reach.[87] In the final rule, DHS modified its original position by allowing other agencies to accept and submit critical infrastructure information to the Program Manager's Office at DHS, but that only that office would have the authority to validate information as protected critical infrastructure information.[88]

The DHS definition of what constitutes a voluntary submission is so scant as to be non-existent. The final regulations say only that whether the submission was voluntary or involuntary will be determined at the time the request for protected status is reviewed. What this means in practice is further explicated in the regulation's discussion of when information might lose protected status. The interim rule provided that protected status could be lost if the Program Manager determined that "the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation." In the final rule, two of these criteria were deleted. DHS dropped the status for information that was publicly available through legal means, explaining that "the CII Act does not provide for a change in status on this ground."[89] The criterion for loss of protection if "required to be submitted to DHS by Federal law or regulation" was also deleted. The rule explained that the "definition of 'voluntary or voluntarily' refers expressly to the time of submittal and is thus retrospective only. This does not, of course, prevent DHS from using current or future authority to mandate submission of any information."[90] In essence, the existing test seems to be one based on "I'll know it

82 Cong. Record, Mar. 15, 2005, p. S2735.
83 S.R. 849, § 12, Accessibility of Critical Infrastructure Information, (a)(1),(2) and (4).
84 68 Fed. Reg. 18523 (Apr. 15, 2003).
85 69 Fed. Reg. 8074 (Feb. 20, 2004).
86 71 Fed. Reg. 52261 (Sept. 1, 2006).
87 *DHS Proposal on CII Attracts Comments on Both Sides of Issue*, Access Reports, v. 29, n. 17, Sept. 10, 2003.
88 71 Fed. Reg. 52263 (2006).
89 *Ibid.*, 52265
90 *Id.*

when I see it," rather than any objective standard. Although the voluntary submission standard from *Critical Mass* is not terribly requester-friendly, at least there is some substantive guidance as to what constitutes a voluntary submission. Under that test, which refers predominantly to submissions made pursuant to a government contract, most submissions a company provides to bid on a contract are deemed mandatory because they are required to successfully bid on the contract.

An article in *SecurityFocus*[91] looked at how the submission process has worked so far and noted that at least the information technology industry is still wary of the program and has yet to submit any information. Although the information is protected from public disclosure, industries are more concerned about its potential wide dissemination within government. Sean Moulton, a policy analyst at the public interest group OMB Watch, explained to *SecurityFocus* the concerns of the public interest community. He indicated that industry had been given more protection than public interest groups thought was warranted, yet industry was still uncomfortable submitting such information. He pointed out that "I really find it troubling that it's industry driving the process and not the government driving the process, when it's the public who has a stake in this. It's the public who will be harmed if these infrastructures are attacked."[92] What the government hoped was an ironclad protection to encourage businesses to share information about vulnerabilities with the government has so far turned out to be a pyrrhic victory at best. It is not the disclosure of the information to the public that scares business as much as it is the sharing of such information within government itself.

The Card Memo

It is important to understand the immediate evolution of information policy after September 11. Perhaps the most dramatic enunciation of where the Bush administration was headed was a White House memo that came to be known as the Card Memo. In March 2002, then White House Chief of Staff Andrew Card sent a memo[93] to all agencies concerning the need to safeguard sensitive but unclassified information pertaining to homeland security. Because such undefined information did not qualify for classification on national security grounds, Card attached two short memos from Laura Kimberly, Acting Director of the Information Security Oversight Office,[94] and Richard Huff and Daniel Metcalfe, Co-Directors of the Justice Department's Office of Information and Privacy,[95] explaining possible FOIA exemptions that could be used to withhold such information. Primary among them was Exemption 2, which allows an agency to withhold records "related solely to the internal personnel rules and practices of an agency." Over the years, courts have stretched these words so they now allow an agency to withhold records where disclosure could lead to circumvention of a law or regulation. The Justice Department memo reminded agencies to consider using Exemption 2 for such sensitive but unclassified information on the untried theory that disclosure would allow a requester to circumvent a law or regulation. Although it said little about the scope of the problem, the Card memo was the first White House policy directive concerning the need to protect sensitive unclassified information and was certainly a primary factor in moving the development of such policies forward.

91 Poulsen, Kevin, *U.S. Info-Sharing Initiative Called a Flop*, SecurityFocus, Feb. 11, 2005.
92 *Ibid.*

93 Andrew H. Card, Jr., Assistant to the President and Chief of Staff, *Memorandum for the Heads of Executive Departments and Agencies*, Subject: Action to Safeguard Information Regarding Weapons of Mass Destruction & Other Sensitive Documents Related to Homeland Security (Mar. 19, 2002) [hereinafter Card memo].
94 Laura S. Kimberly, Acting Director of the Information Security Oversight Office, *Memorandum for Departments and Agencies* (Mar. 19, 2002).
95 Richard Huff & Daniel Metcalfe, Co-Directors, Office of Information and Privacy, Department of Justice, *Memorandum for Departments and Agencies* (Mar. 19, 2002).

Other Information Protection Measures: Sensitive Security Information

Sensitive security information is one of the few such categories with a statutory basis. In November 2001, Congress passed the Aviation and Transportation Security Act, creating the Transportation Security Administration. That statute defines sensitive security information as information describing air carrier screening procedures, airport or air carrier security programs, maritime transportation security procedures, or other related transportation security matters. It prohibits the disclosure of such information if the TSA Administrator determines disclosure would "be detrimental to the safety of passengers in transportation."[96] The Homeland Security Act of 2002 expanded this to cover information that "would be detrimental to the security of transportation." A May 2004 *Federal Register* notice set out 16 categories of information from traditional security plans to security directives and included "other information" that TSA at its discretion determined should be withheld. This statutory authority is structured so that it qualifies as an Exemption 3 statute under FOIA.

These sensitive security information provisions have been involved in a number of incidents that have received national press coverage, including the refusal of TSA staff to allow former Rep. Helen Chenoweth-Hage to board a flight because she refused to submit to a pat-down search and asked for the legal authority to conduct such a search, a request that was denied. Other high-profile incidents involved a lawsuit by activist John Gilmore, after TSA again refused to disclose its authority for demanding personal identification before boarding a flight; Gilmore's suit was ultimately dismissed for lack of standing.[97] A lawsuit was also filed by the ACLU of Northern California on behalf of several people who were told they were on the "No Fly List," but were denied any information concerning why they were put on such a list. Although the judge hearing the lawsuit initially told TSA that it had failed to substantiate its claims, he ultimately ruled that the information was exempt under FOIA.

Critical Energy Infrastructure Information

The Federal Energy Regulatory Commission has created its own category of sensitive information, known as critical energy infrastructure information, and has faced its own specific problems which it has had to finesse. The Commission oversees the energy industry and holds a number of administrative proceedings involving companies and utilities in that area. As a part of these hearings, the Commission requires submission of technical information, including infrastructure information. Generally, most of this information would be public when used in a proceeding. However, after September 11, FERC moved more aggressively than virtually any other agency to remove critical energy infrastructure information from the public domain. The agency's regulations define CEII as information that is exempt from FOIA and submitted to the agency by private parties about proposed or existing critical infrastructure that relates to the production, generation, transportation, transmission or distribution of energy and which "could be useful to a person planning an attack on critical infrastructure."[98]

The most glaring problem with FERC's policy is that it is based on the assumption that this information is exempt from disclosure under FOIA. However, FERC's claims are based not on any court-accepted interpretation of FOIA, but on the Justice Department's suggested potpourri of possible exemptions. These include Exemption 2, which protects information the disclosure of which could allow someone to circumvent a law or regulation, Exemption 7(E), which allows a law enforcement agency to withhold information

96 49 U.S.C. § 114(s)(1) and 49 U.S.C. § 40119(b)(1).

97 *Gilmore v. Gonzales*, 435 F.3d 1125 (9th Cir. 2006), *cert. denied*, 127 S.Ct 929 (2007).

98 18 C.F.R. § 388.113(c) (68 Fed. Reg. 9857, 9870 (March 3, 2003)).

that would reveal investigative methods and techniques, and Exemption 7(F), which allows a law enforcement agency to withhold information the disclosure of which could endanger the physical safety of an individual. The agency also suggested that the information could be withheld under Exemption 4, which protects confidential business information, because a terrorist attack would clearly cause a company economic harm. The other problem is that FERC wanted to continue to share this information during its proceedings, requiring it to create a non-FOIA process of disclosure to those parties with a "need to know," which required parties to sign a non-disclosure agreement. It is difficult to see how information that was previously public could become non-public based solely on agency regulations.

Case Law

There is surprisingly little case law on this subject and so far there are only two state cases that directly deal with aspects of protected CII and what that status might mean for disclosure of the information. In a case in New Jersey where a plaintiff had been denied access to a topographic map in digital form maintained by the Brick Township Municipal Utilities Authority, the appellate court agreed with the state's Government Records Council that the topographic map was exempt from disclosure under the Open Public Records Act because it had been submitted to DHS and been validated as protected critical infrastructure information. The court noted that "BUTMA's GIS topographical mapping data in digital format comes within the definition of 'government record' in [the OPRA]. However, the same information has been found by the DHS to be protected from disclosure by the [Critical Infrastructure Information Act]." The court continued: "BTMUA submitted the electronic GIS data to DHS, obtained confirmation that the data had been received and was presumed protected and finally was informed that the data was validated as PCII. Clearly, information validated as 'PCII shall be treated as exempt from disclosure under the Freedom of Information Act and any State or local law requiring disclosure of records or information.'"[99]

In the second case, the California First Amendment Coalition brought suit against Santa Clara County after it was denied access to the county's GIS basemap in digital form. While the litigation involved several separate exemptions under the California Public Records Act, one claim the county made was that the information was exempt because it was protected as critical infrastructure information under the CIIA. Rejecting that claim, the trial court indicated that:

> [T]he court has considered whether County can cloak the entirety of the GIS basemap with the broad brush protection of CII/PCII simply by depositing it with the federal or state [Office of Homeland Security]. The action taken by County may well be legitimate with regard to some of the information in the GIS basemap, i.e. water lines for delivery of water from Hetch Hetchy, but do not appear to be valid for information that is public record and which have nothing to do with critical infrastructure. For example, information about the assessed value of a single family home in San Jose has nothing to do with critical infrastructure, but because it is contained in the GIS basemap, is it thereby cloaked with the protection of CII/PCII simply by submission to the OHS? It appears County has belatedly focused on the information pertaining to 'water lines' and used that as its primary, if not sole, basis for obtaining the CII/PCII designation without any concession that the GIS basemap consists of any other publicly available information. County's argument runs counter to its earlier argument that CFAC has alternative means of obtaining the same infor-

99 *Tombs v. Brick township Municipal Utilities Authority*, WL 3511459 (N.J. Super. A.D.) (Dec. 7, 2006).

> mation contained in the GIS basemap – if CFAC can obtain, for instance, property assessment data from the assessor's office, County is hard pressed to argue that this same information is now exempt because it has been submitted as CII.

Saying that the county bore the burden of proving that the information was CII, the court observed that "[c]ounty has not make the initial effort to establish that all information contained in the GIS basemap is CII. Having failed to meet its initial burden, County's assertion of this particular exemption fails."[100]

The analysis contained in these two cases does not provide much to go on. In the New Jersey case, the court seems to have taken the position that once DHS designates information as PCII, it is categorically exempt, while the California court believed that the county was required to show in the first instance that all the information was eligible for PCII designation, at least where there were serious doubts as to whether some of the information could be CII since it was already public.

The Impact on Disclosure of Such Categories of Information

These ill-defined categories—be they "sensitive but unclassified," "sensitive security information," or some form of "critical infrastructure information"—almost always do more harm than good. They are a solution to a problem that may not even exist and are based on an antithetical proposition in our democracy—that, when in doubt, always favor secrecy over openness. That is not to say that some government information should not remain secret; we can all agree that some information, such as troop movements in time of war, for instance, should be kept secret. But when our government fosters the attitude that there are vast undefined categories of information that must be, at a minimum, safeguarded by agencies, it does a grave disservice to the ideal of an open democratic society. It is paternalistic for government to assume that people cannot assess and use such information responsibly.

Government officials say these designations, like "sensitive but unclassified," or "for your eyes only," have no legal status and cannot be used to deny access under FOIA. While this is true on a technical level, it is hard to believe that when agency personnel are faced with a document with such a designation they are not going to think twice before agreeing to disclose such a document. In other words, such a designation sets off red flags that suggest the record merits withholding. The problem with the Justice Department's memo attached to the Card memo is that it outlines a strategy for withholding information that perhaps should have been released. When a record says "sensitive, but unclassified," the first step for agency personnel is likely to try to figure out which FOIA exemption can be applied.

For years, most outside observers have complained that too much information is classified. The annual reports of the Information Security Oversight Office consistently show that the number of classification determinations, whether at the original or derivative level, continue to go up every year. But the national security classification scheme provides several potential remedies for forcing the disclosure of classified information. These include a mandatory declassification review, most often in conjunction with an FOIA request, or a review by the Interagency Security Classification Appeals Panel (ISCAP). Review by ISCAP, created by Executive Order 12958 issued by President Clinton, has resulted in further disclosure of previously classified information in a significant majority of cases. However, the number of cases heard by the panel is relatively small and resort to it is not a practical option for many requesters.

100 *California First Amendment Coalition v. County of Santa Clara*, No. 1-06-CV-072630, California Superior Court, County of Santa Clara, May 18, 2007.

When it comes to critical infrastructure information, however, the CIIA has adopted such a broad test that it allows information to be completely exempt from public disclosure regardless of its content if the submitter can get DHS to validate it as protected critical infrastructure information. There is no nod to any public interest or responsible alternative uses of the information. Information that has been public previously can now become completely non-public merely because DHS decides that its designation as protected critical infrastructure information is desirable. The CIIA is an extension of secrecy policies that have existed for years in the U.S. judicial system, allowing litigants to seal or protect records that may have substantial significance to public safety or public policy. The idea that secrecy is the best remedy betrays democratic principles and narrows the ability to use information to such an extent that much of its utility is completely lost. A policy like the CIIA is based on the premise that government can enlist the cooperation of information holders by providing confidentiality. But this system seems to have largely backfired in the area of critical infrastructure information because business is more fearful of government than it is of public disclosure. In other words, the carrot provided to encourage submission is not nearly large enough and is not even aimed at the actual problem. Beyond that, the over-arching policy underlying government access to critical infrastructure information is undercut by the CIIA. If there is indeed a need for government to know about the vulnerabilities of the critical infrastructure so that it can prepare for a potential terrorist threat, then government needs to mandate disclosure of such information, not make it voluntary in a system that doesn't provide sufficient rewards in the first place. By taking that tact, the federal government has gotten the worst of both worlds. It has ensured that critical infrastructure information is not available to the public while failing to secure its availability to the government at the same time.

The protection of critical infrastructure information is premised on the idea that by protecting such information from would-be terrorists we take steps to protect ourselves from such terrorism. But unless we could keep all information about any vulnerable man-made or natural potential target from anyone and everyone, which is clearly impossible and not even contemplated, there is sufficient information for a would-be terrorist to conclude that breaching a dam or blowing up a major bridge would probably have catastrophic consequences. Further, because the policy assumes the continued vulnerability of the infrastructure, its blanket exemption for public access prevents informed public discussion and political debate concerning how best to remedy existing vulnerabilities. If a bridge is unsafe or an urban chemical plant is a significant environmental hazard, such problems are more likely to be remedied if public and political pressure is brought to bear. Withholding any debate on such issues is tantamount to ensuring that such vulnerabilities are accepted as the status quo rather than being subject to a remedy.

When it comes to these undefined categories of information there are no remedies short of litigation, probably under FOIA. While the government's collection of recommended exemptions has not been thoroughly tested, at least two U.S. district court judges have accepted some combination of these claims.[101] Further, the expanded deference shown by the D.C. Circuit in litigation[102] over disclosure of the identities of individuals who were detained in the immediate aftermath of September 11, 2001, suggests that courts would likely be sympathetic to the government's arguments when it came to withholding information based on concerns about possible terrorist use. There is no administrative appeal aside from that available under FOIA. This means, realistically, that there are fewer checks against the improper denial of

101 *See Living Rivers, Inc. v. Bureau of Reclamation*, No. 2:02-CV-644TC (D. Utah, Mar. 25, 2003); *Coastal Delivery Corp. v. Customs Service*, No. 02-3838 WMB (C.D. Cal., Mar. 14, 2003).

102 *Center for National Security Studies v. DOJ*, 331 F.3d 918 (D.C. Cir. 2003).

such undefined categories of information than exist for classified national security information.

Further, remedies to challenge the designation of such information must be made available. Requesters must not be forced to go to court as their only alternative. Instead, a process akin to mandatory declassification review should be instituted. Along these same lines, time limits for protection should be considered and implemented. Sensitive information may well be sensitive for a period of time and lose its sensitivity thereafter. Once information is no longer sensitive it should be made publicly available.

The obsession with protecting such information because under some scenario it might be of use to a terrorist, fails to consider the value of the information itself. Vulnerabilities in our infrastructure should not be broadcast to potential enemies, but should not be hidden under a basket either. A good analogy for fostering greater public disclosure is how open source software code works in the computer world. When such code is openly available, individuals tinker with it in an effort to improve it or to expand its utility. When such programs are closed, they stagnate rather than expand. Bridges or roads or manufacturing facilities that are vulnerable will not be fixed because their vulnerabilities are hidden. They are much more likely to be fixed, and thus become less useful as an end goal for terrorists, because individuals and groups put pressure on government or business to fix them. We need to be less fixated on the potential harmful use of information and more cognizant of the way in which we can use that information to achieve a result that makes us both safer from potential attack and safer because vulnerabilities have been addressed. As a nation we cannot very well address vulnerabilities when we do not know they exist.

These undefined categories of information stifle the availability and use of information. They expand the universe of information agencies are likely to withhold from the public solely because of their designation. They also restrict the availability of information within government and particularly between levels of government. One of the lessons of the 9/11 Commission's report is that information is most useful when it is available. Various bureaucratic gate-keeping regimes that slow or halt the flow of information, or worse still, hide its existence, are detrimental to our available knowledge base and, ultimately, do us more harm than good.

2.4 Protecting Sensitive Information: Critical Infrastructure Protection at the Local Level

by Maeve Dion

Abstract

Given the upsurge in the use of security rationales as justifications for non-release decisions regarding freedom of information requests related to critical infrastructure, some people are asking whether we should have a common definition for such assessments. This article discusses the background to this debate and ultimately concludes that (a) in the current circumstances of both vague and complex federal guidelines, and (b) with the necessity of analyzing these issues from a state and local perspective, such a common-language policy may not be very useful.

Background of Critical Infrastructure Protection

This conference focuses on the time period after September 11, 2001, but it should be noted that the concept of critical infrastructure protection (CIP), although perhaps not labeled as such, has a long history and did not develop only in response to what we may now call terrorist incidents. Although CIP reflects a fear of foreign enemies attacking domestic assets, CIP also incorporates threats from native saboteurs and from nature (under current terminology, this is an "all hazards"

approach). While the depth and breadth of CIP history varies depending on the industry sector, a few examples can demonstrate the pre-1990s awareness of CIP:

- In the World War One and World War Two eras, the United States instituted civil defense programs, which related directly to the fear of domestic invasion by our respective nation-state enemies.[103]
- In the 1960s, the Defense Electric Power Administration recognized that public access to information about power systems (specifically, maps of the power grids) could endanger the industry and everything reliant on it. This awareness in part arose because of various threats and incidents of sabotage, such as when domestic political protestors disabled electricity transmission lines in Colorado.[104]
- By the 1980s, the Department of Energy was issuing terrorist threat advisories to the electricity industry; the Department of Justice was assembling a critical asset database and a communications/coordination system in conjunction with the private owners and operators; and the Department of Defense for the first time stated that its highest priority was the assurance of energy supply to its essential facilities.[105]
- In 1986, the National Security Council directed FEMA "to identify the extent to which various critical infrastructure elements (e.g., the computerized banking system, power grids, and communication networks) were vulnerable to terrorism and propose near and long term solutions."[106]
- After a 1989 California earthquake, gas companies were hindered in restoring gas service because the phone company shut off phone services that were needed for the gas companies' restoration activities.[107] This incident showed not only the problems of interdependencies, but also highlighted the need—within both the private and public sectors—for awareness of such interdependent systems and functions.

Two evolutions furthered the recognition of the importance of CIP: the increasing government reliance on private sector suppliers, and the development of computers and the information age. While the early age of CIP focused primarily on preventing a physical attack through conventional means, CIP now incorporates a spectrum of threats, including attacks that target, or are accomplished via, complex cyber systems.

The first major policy document on CIP, and the vulnerabilities enhanced by the information age, was the 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP).[108] Since then, there have been numerous CIP offices established (and renamed and reformed) at the federal, state, and local levels of government, as well as within research institutions; and there have been various laws and regulations relating to CIP. It should also be recognized that much of CIP may not be labeled as "critical infrastructure protection"—just as "Homeland Security" incorporates numerous legacy agencies and historical concepts and policies, so does CIP. Thus, a 2006 search of the term "critical infrastructure" in online Westlaw and Lexis legal databases (state and federal cases, no date limitations), resulted in only 42 cases[109] . . . and only three of these cases used

103 *See* Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States,* 7-8 & 22-23 (2006) (discussing efforts of the Council of National Defense and the Federal Civil Defense Administration).

104 *Id.* at 51, 60.

105 *Id.* at 58.

106 *Id.* at 71 n.iv (quoting a 1989 Secret Service report by Charles Lane to the U.S. Senate Committee on Governmental Affairs).

107 *Id.* at 110.

108 *Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection (1997).

109 The most recent searches were conducted on November 6, 2006. The searches resulted in 43 and 45 opinions respectively; however some cases had several

the phrase "critical infrastructure" (CI) in the manner used in this paper.

Thirty-one of the cases used the phrase in reference to physical infrastructure improvements (e.g., the building of roads).[110] Two cases mentioned damage to CI as a statutory factor for increasing sentencing,[111] and six cases merely mentioned CI as part of a governmental office title (e.g., Public Safety and Critical Infrastructure Division),[112] or to identify critical equipment or facilities,[113] and in these cases, CIP was unrelated to the disputes. Of the three CIP-relevant cases, one case sustained the constitutionality of random searches in the New York subway system;[114] one case held that the District of Columbia's attempt to regulate the rail transportation of hazardous materials through D.C. was preempted by federal law;[115] and one case exempted U.S. Bureau of Reclamation maps from disclosure under the federal Freedom of Information Act because release of the maps could increase the risk of terrorist attacks.[116]

It should be noted, however, that numerous cases have addressed aspects of CIP without explicitly referencing "critical infrastructure" (both pre- and post- September 11, 2001). Some of the components of CI are protected by government regulations or criminal laws specific to an industry or act, rather than general CIP; for example, although the Computer Fraud and Abuse Act[117] does not specifically mention "critical infrastructure" or municipal radio systems, that was the law used to convict an individual who intentionally disrupted a city's emergency response radio communications system—a system that would definitely be considered a component of CI.[118] [Note that Congress has recently enacted a few industry-specific CIP laws, which resulted from concerns that the respective industries and regulators had not been moving quickly enough to institute adequate protection measures under the more amorphous CIP definitions and legislation discussed below.[119]]

What Infrastructure is Critical?

This question of what constitutes CI is often the crux of many debates relating to freedom of information (FOI) non-disclosure decisions based on CIP concerns. Formal governmental definitions of CI can be traced back to the 1996 PCCIP Executive Order, which defined infrastructure as "[t]he framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole."[120] This Executive Order specifically recognized that some infrastructures were *critical*: "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[121]

A few years later, Congress responded to the September 11, 2001, terrorist attacks by passing various new laws, including the Critical Infrastruc-

opinions.

110 *E.g., Banner v. U.S.*, 303 F. Supp. 2d 1 (D.D.C. 2004), *aff'd*, 2005 U.S. App. LEXIS 23828 (D.C. Cir. 2005).

111 *E.g., U.S. v. Al-Rekabi*, 454 F.3d 1113 (10th Cir. 2006).

112 *E.g., Nat'l Sci. & Tech. Network, Inc. v. FCC*, 397 F.3d 1013 (D.C. Cir. 2005).

113 *E.g., Former Employees of I.B.M. v. Sec'y of Labor*, 403 F. Supp. 2d 1311 (Ct. Int'l Trade 2006).

114 *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006).

115 *CSX Transp. v. Williams*, 406 F.3d 667 (D.C. Cir. 2005).

116 *Living Rivers v. Bureau of Reclamation*, 272 F. Supp. 2d 1313 (D. Utah 2003).

117 Codified at 18 U.S.C. § 1030.

118 *U.S. v. Mitra*, 405 F.3d 492 (7th Cir. 2005).

119 For example, the 2005 Energy Act contained provisions mandating electric reliability standards, 16 U.S.C. § 824o, and in October of 2006, Congress required increased CIP in chemical facilities, Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, § 550 (2006).

120 Exec. Order No. 13010, 60 Fed. Reg. 37347 (July 17, 1996).

121 *Id.*

tures Protection Act, in which Congress explicitly found that "[p]rivate business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors."[122] Congress defined "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[123]

These definitions are quite broad, and are not further defined in any piece of legislation (although individual agency regulations may provide more specific guidance within their jurisdictions).[124] Congress increased the complexity of CI definitions in the Homeland Security Act of 2002, where it differentiated "critical infrastructure" from "key resources," which was defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government."[125] Within the realm of national U.S. infrastructure, this is the guidance for determining which should be considered critical, and therefore which should receive the focus of federal CIP efforts and information protection.

Many states have passed their own laws to protect CI and related sensitive information. For example, in 2003 Virginia enacted a law that added critical infrastructure and vulnerability assessments to an exemption in the state FOI act. The current exemption (resulting from the 2003 law and amendments in intervening years) permits the withholding of:

> Plans and information to prevent or respond to terrorist activity, the disclosure of which would jeopardize the safety of any person, including (i) critical infrastructure sector or structural components; (ii) vulnerability assessments, operational, procedural, transportation, and tactical planning or training manuals, and staff meeting minutes or other records; and (iii) engineering or architectural records, or records containing information derived from such records, to the extent such records reveal the location or operation of security equipment and systems, elevators, ventilation, fire protection, emergency, electrical, telecommunications or utility equipment and systems of any public building, structure or information storage facility, or telecommunications or utility equipment or systems. The same categories of records of any governmental or nongovernmental person or entity submitted to a public body for the purpose of antiterrorism response planning may be withheld from disclosure if such person or entity in writing (a) invokes the protections of this subdivision, (b) identifies with specificity the records or portions thereof for which protection is sought, and (c) states with reasonable particularity why the protection of such records from public disclosure is necessary to meet the objective of antiterrorism planning or protection. Such statement shall be a public record and shall be disclosed upon request. Nothing in this subdivision shall be construed to prohibit the disclosure of records relating to the structural or environmental soundness of any building, nor shall it prevent the disclosure of informa-

122 Pub. L. No. 107-56, § 1016(b)(2) (2001) (prior to 2006 reauthorization) (the Critical Infrastructures Protection Act of 2001 was also enacted as part of the USA PATRIOT Act of 2001).

123 *Id.* at § 1016(e).

124 *E.g.*, 49 C.F.R. § 1520 *et seq.* (Transportation Security Administration regulations regarding the Protection of Sensitive Security Information).

125 Homeland Security Act of 2002 §§ 2(9), 2(15)(A)(i), 6 U.S.C §§ 101(10), 101(15)(A)(i) (as amended); *see also* John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*, p. 7 (Oct. 1, 2004) (CRS Report for Congress Order Code RL32631).

> tion relating to any building in connection with an inquiry into the performance of that building after it has been subjected to fire, explosion, natural disaster or other catastrophic event.[126]

As demonstrated by these examples of Virginia state law and the federal experience, the term "critical infrastructure"—all that CI may, or may not, encompass—is highly relevant (and greatly debated) in the FOI context. In addition to laws like this Virginia state FOI exemption (and other states' similar laws with descriptive rather than categorical/classification exemptions), information may be withheld from public disclosure because the information is deemed Critical Infrastructure Information (CII), Sensitive Security Information (SSI), or Homeland Security Information (HSI).[127] Also, in addition to the more traditional classifications of Top Secret, Secret, and Confidential, information may be labeled For Official Use Only (FOUO) or Sensitive but Unclassified (SBU), and may thus be prohibited from certain transfers or disclosures. And to further complicate the issue, these terms can have different definitions not only among federal agencies, but also within different state and local governments. When it comes to applying these labels and categories and descriptive state non-disclosure laws on a case-by-case basis in the context of FOI requests, the crux of the security-versus-openness debate is truly a matter of perspective.

The Problem of Perspective

When a government entity decides to withhold information—whether under a CI exemption in a FOI law, or under a law protecting CII or HSI information—that entity does so on a case-by-case basis, on its own determination regarding both the criticality of the infrastructure and the sensitivity of the information being requested. These determinations may vary greatly among government bodies, depending on each entity's perspective of what is "critical" to that locality or to that specific government.

For example, what is critical to a city may not be critical to the nation, to a region, or even to the respective state. A city government may thus be concerned about protecting systems or assets that are "so vital to the ~~United States~~ *city* that the incapacity or destruction of such systems and assets would have a debilitating impact on security, ~~national~~ *local* economic security, ~~national~~ *local* public health or safety." Security and public health and safety are inherent responsibilities of government; determinations of the criticality of the infrastructures within a jurisdiction depend on the risk calculations regarding the likelihood of the threat and the weight of the responsibility (how great is the potential damage, based upon the level of vulnerability and the type and quantity of damage). If the disclosure of certain information could increase either the likelihood of harm or the consequential damage, the government may decide that one of its responsibilities is to restrict access to that information.[128]

If the information is general public knowledge, then obviously most FOI laws and non-release exemptions will not apply. However, if information is public, but not necessarily readily available, the government may still choose to withhold the information if it deems that greater access to the information may increase either the amount of damage or the likelihood of harm. Here, one government concern is that, while there may be some risk in maintaining the information in the public domain, that risk is limited if it is not widely or easily accessible by those who may want to use

126 Va. Code Ann. §§ 2.2-3705.2(4) (updated July 2, 2007).

127 For an overview of the protection of private sector information in the context of the Federal FOIA, SSI and other federal CII protection laws, see James W. Conrad, *Protecting Private Security-Related Information from Disclosure by Government Agencies*, 57 Admin. L. Rev. 715 (2005).

128 *E.g., Living Rivers, Inc. v. United States Bureau of Reclamation*, 272 F. Supp. 2d (D. Utah 2003).

the information to cause harm.[129] For example, a municipality may choose to withhold full access to geographic information systems (GIS) that map utility systems and access points . . . even though anyone could walk through the town and note the location of utility manholes.[130]

The local government's thoughts may somewhat follow these lines: (a) if saboteurs wanted to target a U.S. municipality via its utility systems, the bad guys are more likely to pick a town that allows for easy access to its utility information; (b) if saboteurs still wanted to target our municipality, even without such easy information access, the necessity of the bad guys tromping through the streets of the town with a laptop (or notebook and pencil), jotting down all the utility info they can see, provides a greater likelihood of detection and prevention, or at least a chance for prosecution after an attack if the saboteurs were photographed by any surveillance cameras in the town.

It should be noted that there are two other issues of perspective that a government entity may face when deciding to release information under a FOI request: (1) when the requested information, standing alone, may not be a security threat, but paired with other information, may be deemed a CI threat (i.e., aggregated information); and (2) when the requested information is does not endanger infrastructure within the government entity's jurisdiction, but may imperil another jurisdiction's CI. Thus, in regard to CIP-related FOI requests, non-disclosure determinations are highly complex and may include decisions as to:

- what is critical to *this* jurisdiction;
- what is the likelihood of harm if the information is disclosed;
- does this non-sensitive information become more sensitive when paired with other information;
- what is critical to interconnected and interdependent systems and jurisdictions, and does the release of this information endanger those other constituencies; and
- do any or all of these concerns outweigh our traditional policies of open government?

Further, a state or local government would also have to determine whether the respective CI at issue falls under any federal information-protection laws and regulations, so that even if the state would permit its release, the federal government mandates non-disclosure.

Conclusions

These concerns, and the example of the municipal utility mapping above, may be deemed far-fetched by some people. However, it is the government that has the responsibility of public safety and security, and the government that has a duty to fulfill FOI requirements that relate to its jurisdiction. Therefore it is from that perspective that non-disclosure decisions are being made. As one analyst stated,

> [f]or many years, we have assumed that we could protect people, save lives, reduce in-

129 This concern regarding easier access to and transfer of information in digital format (e.g., via the Internet, with computer mapping tools, etc.) was recognized before the 2001 terrorist attacks; a 1999 federal law restricted electronic release of off-site consequence analyses by chemical companies. However, to maintain traditional concepts of public access to government information, and to retain the incentive for the chemical companies to reduce the likelihood of chemical accidents (via informational openness and potential public pressure), print-outs of the consequence analyses were made available at federal reading rooms throughout the U.S. *See also* David Zocchetti, *Public Disclosure of Information by Emergency Services Agencies: A Post-September 11 Paradigm Shift*, A Legal Guide to Homeland Security and Emergency Management for State and Local Governments, p. 3 (Ernest B. Abbott & Otto J. Hetzel eds., 2005); and Conrad, *supra* note 25, at .740 (briefly discussing FERC's "non-Internet public" information category, which includes public information that is not included in FERC's online records information system).

130 *See, e.g.*, Security Officials Seek to Block Some Online Maps (NPR radio broadcast, Oct. 8, 2007).

> juries, and minimize the impacts to property and the environment by disclosing information . . . This disclosure has been based on two premises: That more information in people's hands will encourage them to take protective measures (strap down their water heaters, move to a safer neighborhood, lobby their planning agencies, etc.), and provide them with a tool to hold their government accountable to addressing the disaster risks around them. With terrorism, however, we may have encountered a risk under which more information in more people's hands may cost more in decreased levels of safety, because our assessments, plans, and many other types of records can be used against us.[131]

As more time passes without CI attacks or increases in threats, local governments may reach different conclusions when balancing security versus openness. Non-disclosure decisions under FOI laws are challengeable; following these administrative procedures, courts may find that, although the government should be granted deference in its security and safety determinations, withholding of some information is no long reasonable—either because the threat environment has changed, or because the subject is not really a matter "critical infrastructure," "sensitive security," or other security information protection category.

For the skeptical, it should be noted that not all courts are overly deferential to arbitrary governmental use of security and CIP rationales in relation to FOI requests/exclusions. For example, the Supreme Court of Virginia recently rejected a municipal airport authority's claim that "federal airport-security laws and regulations preempt the provisions of the [Virginia FOI] Act requiring specific, timely responses and mandate protection of SSI."[132] In that case, the airport authority had failed to follow the state FOI procedures, as it was waiting for legal advice from the federal Transportation Security Administration regarding the petitioner's FOI request.[133] The court agreed with the petitioner's claim that although "airport security is an extremely serious matter since the events of 9/11," the airport authority still had to either prove that all requested documents were protected SSI, or else produce the non-SSI documents, and that these actions had to be accomplished in a timely manner in accordance with the state FOI procedures.[134] Holding that the airport authority had violated the state FOI law, the court reversed the lower court's judgment and granted costs and attorney's fees to the petitioner.[135]

It has only been six years since the 2001 terrorist attacks, and since Congress first defined "critical infrastructure" from a federal perspective. In the immediate aftermath of September 11, 2001, state and local governments had to respond to an upsurge of security and safety fears. In the intervening years, we have all had to wrangle with the concepts of homeland security and critical infrastructure protection.

As one of the PCCIP Commissioners said, "when it comes to critical infrastructure protection the national security pyramid is inverted. . . . The pyramid is stood on its head. The federal government is the least knowledgeable about the inner workings of critical infrastructures, the banking system, electrical power grids, telecommunications networks in an age of convergence."[136] What this Commissioner meant was that the CI owners and operators (mostly the private sector) are more knowledgeable than the federal government in respect to protection of their infrastructures.[137]

131 Zocchetti, *supra* note 27, at 8.

132 *Fenter v. Norfolk Airport Authority*, 649 S.E.2d 704, 709 (Va. Sept. 14, 2007).

133 *Id.* at 706-08.

134 *Id.* at 709.

135 *Id.*

136 David Keyes, Commissioner, President's Commission on Critical Infrastructure Protection, quoted in Brown, *supra* note 1, at 114-16.

137 *Id.*

However, it is equally true that state and local governments are more knowledgeable than the federal government when it comes to determining, for example, (a) whether a specific infrastructure is critical to a region, state, or municipality; and (b) whether the disclosure of certain information impacts that critical infrastructure. Thus, even if arguments for a common CI definition and CIP exemption were successful, this article demonstrates that application of such definitions and exemptions may still result in varying disclosure decisions, based upon the perspectives of the governmental bodies receiving the FOI request. We have a history of using the states as experimental laboratories, where new procedures or laws or policies can be tried out, amended, and refined; very often this approach helps us find the best practices. Perhaps this approach will also prove true in relation to protecting sensitive CI information. If so, rather than calling for a federally-led common CI definition and CIP exemption, we might instead begin a survey of the best practices among state and local FOI-responding offices. If we also look at how these entities make their criticality and risk determinations, not only might such a study be useful for other state and local governments, it might also help us refine our federal practice of protecting CII, SSI, HSI, etc.

2.5 Protecting Sensitive Information: A Private Sector Perspective

by Maeve Dion

Abstract

> "For many years, we have assumed that we could protect people, save lives, reduce injuries, and minimize the impacts to property and the environment by disclosing information…This disclosure has been based on two premises: That more information in people's hands will encourage them to take protective measures (strap down their water heaters, move to a safer neighborhood, lobby their planning agencies, etc.), and provide them with a tool to hold their government accountable to addressing the disaster risks around them. With terrorism, however, we may have encountered a risk under which more information in more people's hands may cost more in decreased levels of safety, because our assessments, plans, and many other types of records can be used against us."[138]

This paper provides a brief background on critical infrastructure protection, and discusses the protection of sensitive critical infrastructure information from a private sector perspective.

Background of Critical Infrastructure Protection

This conference focuses on the time period after September 11, 2001, but it should be noted that the concept of critical infrastructure protection (CIP), although perhaps not labeled as such, has a long history and did not develop only in response to what we may now call terrorist incidents. Although CIP reflects a fear of foreign enemies attacking domestic assets, CIP also incorporates threats from native saboteurs and from nature (under current terminology, this is an "all hazards" approach). While the depth and breadth of CIP history varies depending on the industry sector, a few examples can demonstrate the pre-1990s awareness of CIP:

- In the World War One and World War Two eras, the United States instituted civil defense programs, which related directly to the fear of domestic invasion by our respective nation-state enemies.[139]

138 David Zocchetti, *Public Disclosure of Information by Emergency Services Agencies: A Post-September 11 Paradigm Shift*, A Legal Guide to Homeland Security and Emergency Management for State and Local Governments, 8 (Ernest B. Abbott & Otto J. Hetzel, eds., 2005).

139 *See* Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States,* 7-8 & 22-23 (2006) (discussing efforts of the

- In the 1960s, the Defense Electric Power Administration recognized that public access to information about power systems (specifically, maps of the power grids) could endanger the industry and everything reliant on it. This awareness in part arose because of various threats and incidents of sabotage, such as when domestic political protestors disabled electricity transmission lines in Colorado.[140]
- By the 1980s, the Department of Energy was issuing terrorist threat advisories to the electricity industry; the Department of Justice was assembling a critical asset database and a communications/coordination system in conjunction with the private owners and operators; and the Department of Defense, for the first time, stated that its highest priority was the assurance of energy supply to its essential facilities.[141]
- In 1986, the National Security Council directed FEMA "to identify the extent to which various critical infrastructure elements (e.g., the computerized banking system, power grids, and communication networks) were vulnerable to terrorism and propose near and long term solutions."[142]
- After a 1989 California earthquake, gas companies were hindered in restoring gas service because the phone company shut off phone services that were needed for the gas companies' restoration activities.[143] This incident showed not only the problems of interdependencies, but also highlighted the need—within both the private and public sectors—for awareness of such interdependent systems and functions.

Two evolutions furthered the recognition of the importance of CIP: the increasing government reliance on private sector suppliers, and the development of computers and the information age. While the early age of CIP focused primarily on preventing a physical attack through conventional means, CIP now incorporates a spectrum of threats, including attacks that target, or are accomplished via, complex cyber systems.

The first major policy document on CIP, and the vulnerabilities enhanced by the information age, was the 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP).[144] The Executive Order with established the PCCIP defined infrastructure as "[t]he framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole."[145] This Executive Order specifically recognized that some infrastructures were *critical*: "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[146]

Since the PCCIP, there have been numerous CIP offices established (and renamed and reformed) at the federal, state, and local levels of government, as well as within research institutions; and there have been various laws and regulations relating to CIP. In 1998, Presidential Decision Directive No. 63 (PDD-63) identified principles for protecting the U.S. from cascading disruptions as a result of interdependent critical infrastructure, and guarding against attacks on our information technol-

Council of National Defense and the Federal Civil Defense Administration).

140 *Id*. at 51, 60.

141 *Id*. at 58.

142 *Id*. at 71 n.iv (quoting a 1989 Secret Service report by Charles Lane to the U.S. Senate Committee on Governmental Affairs).

143 *Id*. at 110.

144 *Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection (1997).

145 Exec. Order No. 13010, 60 Fed. Reg. 37347 (July 17, 1996).

146 *Id*.

ogy.[147] PDD-63 also called for a National Infrastructure Assurance Plan, but such a plan was not created for another eight years.

A few years later, Congress responded to the September 11, 2001, terrorist attacks by passing various new laws, including the Critical Infrastructures Protection Act, in which Congress explicitly found that "[p]rivate business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors."[148] Congress defined "critical infrastructure" (CI) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[149]

These definitions are quite broad, and are not further defined in any piece of legislation (although individual agency regulations may provide more specific guidance within their jurisdictions[150]). The Congress increased the complexity of CI definitions in the Homeland Security Act of 2002, where it differentiated "critical infrastructure" from "key resources," which it defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government."[151]

Protecting Sensitive Information

The government traditionally controls certain aspects of CIP, such as those related to national defense, law enforcement, and foreign intelligence and affairs. However, the majority of U.S. infrastructure is owned or operated by the private sector. In the words of one of the PCCIP Commissioners,

> when it comes to critical infrastructure protection the national security pyramid is inverted….The pyramid is stood on its head. The federal government is the least knowledgeable about the inner workings of critical infrastructures, the banking system, electrical power grids, telecommunications networks in an age of convergence. The owners and operators of the business are the best informed, the most knowledgeable and the most capable of dealing with emergencies . . . So this inversion of the national security pyramid is one that, in my mind, very much argued against attempting to impose from the unknowledgeable government sector onto the very knowledgeable and capable private sector what [CIP] criteria should be put in place. I think the majority of [the PCCIP Commissioners] agreed that the government didn't know enough about what it was doing to be entrusted with legislating that sort of response."[152]

Thus, the PCCIP recommended that the government institute programs to garner information from the CI owners and operators. Following this recommendation, and in order to effectuate CIP under the mandates of the Homeland Security Act, the Department of Homeland Security (DHS) has created numerous different programs for "in-

147 Presidential Decision Directive/NSC-63. May 22, 1998.

148 Pub. L. No. 107-56, § 1016(b)(2) (2001) (prior to 2006 reauthorization) (the Critical Infrastructures Protection Act of 2001 was also enacted as part of the USA PATRIOT Act of 2001).

149 *Id*. at § 1016(e).

150 *E.g*., 49 C.F.R. § 1520 *et seq*. (Transportation Security Administration regulations regarding the Protection of Sensitive Security Information).

151 Homeland Security Act of 2002 §§ 2(9), 2(15)(A)(i), 6 U.S.C §§ 101(10), 101(15)(A)(i) (as amended); *see also* John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*, 7 (Oct. 1, 2004) (CRS Report for Congress Order Code RL32631).

152 David Keyes, Commissioner, President's Commission on Critical Infrastructure Protection, quoted in Brown, *supra* note 2, at 114-16.

formation sharing" and "public-private partnerships." On one hand, DHS was attempting to get a lot of CI information from the private sector; on the other hand, the private sector wanted certain pieces of intelligence information in order to determine national security risks to their own infrastructures.

The information sharing programs have had a mixed result for various reasons—of course, the government was wary of sharing intelligence information, but the private sector, too, was concerned with the detrimental effects that may accompany increased private sector information collating and transfer to the government. Private companies may face economic and competition harms if they share vulnerability information. As one PCCIP Advisory Group Member stated, "it's an act against nature for a company to sit down with its competitors and share its vulnerabilities and to share information which is going to give its competitors competitive advantages."[153] Companies also want to limit costly regulation, and are thus unlikely to give the government any more information than necessary. Further, once proprietary commercial information is in the hands of government, it may be accessible through freedom of information (FOI) laws, which could not only hinder the private companies' competitiveness, but could expose CI vulnerabilities to malfeasors, thus heightening risks of sabotage.

Some of the security concerns and information sharing problems may be addressed by laws that restrict the use of and access to sensitive information—for example, FOI exemptions, the federal Protected Critical Infrastructure Information (PCII) Program, and the new Critical Infrastructure Partnership Advisory Council, which DHS established as a committee exempt from the public access/notice requirements of the Federal Advisory Committee Act.[154] Information may be withheld from public disclosure because the information is deemed Critical Infrastructure Information (CII), Sensitive Security Information (SSI), or Homeland Security Information (HSI).[155] Also, in addition to the more traditional classifications of Top Secret, Secret, and Confidential, information may be labeled For Official Use Only (FOUO) or Sensitive but Unclassified (SBU), and may thus be prohibited from certain transfers or disclosures. And to further complicate the issue, these terms can have different definitions not only among federal agencies, but also within different state and local governments.

The multitude of classifications, and the varying definitions for similar terms, can cause confusion regarding a government office's responsibility as to disclosure decisions. As stated in a January 2007 report by a Department of Defense (DoD) federal advisory committee,

> [a] particularly thorny issue is the lack of guidance from DHS. DHS currently relies on the classification guidance of other agencies (DoD and [the Department of Energy], in particular). In addition, the "sensitive but unclassified" category of information for DHS requires careful review and implementation of the proposed Sensitive Homeland Security Information since it will be the official interface to state, local, tribal, and some private sector entities. . . . Certainly the issue of how much information the Federal Government really needs for homeland security, how to protect that information, and how to share it appropri-

153 Brown, *supra* note 2, at 155 (quoting Jamie Gorelick, Co-Chair of the PCCIP Advisory Committee).

154 *See* Brett Callahan, whitepaper, *Listening to the Eighty-Five Percent: the Federal Advisory Committee Act and Communication Between the Private Sector and the Department of Homeland Security* (2005), available at http://cipp.gmu.edu/archive/FACA.pdf.

155 For an overview of the protection of private sector information in the context of the Federal FOIA, SSI and other federal CII protection laws, see James W. Conrad, *Protecting Private Security-Related Information from Disclosure by Government Agencies*, 57 Admin. L. Rev. 715 (2005).

> ately, were all open questions at the time this Task Force concluded."[156]

In addition to the quantity and variety of classifications, when it comes to applying classification labels and informational categories on a case-by-case basis in the context of FOI requests, the crux of the security-versus-openness debate is truly a matter of perspective. When a government entity decides to withhold information—whether under a CI exemption in a FOI law, or under a law protecting CII or HSI information—that entity does so on a case-by-case basis, on its own determination regarding both the criticality of the infrastructure and the sensitivity of the information being requested.

These determinations may vary greatly among government bodies, depending on each entity's perspective of what is "critical" to that locality or to that specific government. For example, what is critical to a city may not be critical to the nation, to a region, or even to the respective state. A city government may thus be concerned about protecting systems or assets that are "so vital to the ~~United States~~ *city* that the incapacity or destruction of such systems and assets would have a debilitating impact on security, ~~national~~ *local* economic security, ~~national~~ *local* public health or safety."

These are the kinds of decisions that are not only necessary to preserve the balance of security and openness in government, but such determinations are also needed to inform the private-sector businesses that own and operate our critical infrastructure. One of the important needs in business is clarity of expectations; some degree of predictability is necessary for internal corporate decision-making. For example, a business needs to be able to anticipate what may be considered a public record/document for FOI purposes; what will likely be covered in a FOI exemption; and, if there is an exemption for voluntarily-shared CI information, what is the meaning of "voluntarily" in that context. A business should know which government entities hold sensitive information relating to that business; whether those entities operate under FOI rules; and how those entities apply the FOI rules to this kind of information.

It may be thought that if a CI-related business only interacts with a limited number of government jurisdictions, then the tasks of learning and maintaining current answers to these questions is relatively manageable. However, the business may have regional or nationwide (or international) interactions. The business may be deemed a critical infrastructure by another company or system that is dependent on the business, and the dependant company or system may be located in an entirely separate jurisdiction. The business may be deemed "critical" infrastructure by some governmental bodies and not others; or the criticality of the business's assets or services may be fluid (criticality depending upon circumstances). In these situations, it is harder to achieve clarity of expectations.

Thus, in relation to CIP and FOI issues, some of the challenges we are currently faced with include (a) rather vague federal guidelines; (b) a multitude of classifications and definitions among agencies and offices; (c) the necessity of analyzing criticality not only from a federal perspective, but also from state and local perspectives; (d) the complications of interdependencies (e.g., when several governmental bodies may hold information which may only be protected as CI information by one jurisdiction); and (e) the business need for predictability in decisions of nondisclosure and information transfer. In the U.S., we have a history of using the states as experimental laboratories, where new procedures or laws or policies can be tried out, amended, and refined; very often this approach helps us find the best practices. Perhaps this approach will also prove true in relation to protecting sensitive CI information. It may

156 *Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection*, p. 25, United States Department of Defense (January 2007).

therefore be useful to survey the best CIP-related practices among state and local FOI-responding offices. If we look not only at the outcomes but also at how these entities make their criticality and risk determinations, not only might such a study be useful for other state and local governments, it might also help private sector CI owners/operators to make more reliable business decisions regarding expectations of governmental protection of sensitive CI information.

Chapter 3

Public Health

Synopsis

3.1 Informing the Public: Overbroad Secrecy in Public Health

by Rick Blum[1]
Coordinator, Sunshine in Government Initiative[2]

Prior to September 11, the Intelligence Community and the U.S. Government labored to prevent attacks by Osama Bin Laden and his terrorist network against the United States, but largely without the benefit of an alert, mobilized and committed American public.

—Congressional Joint Inquiry into 9/11[3]

Introduction

Democracy lives on openness. But openness is more than a value. It is a tool for strengthening security and advancing science, technology and human knowledge. Secrecy also is an effective, and at times necessary, tool for the government to use in advancing other interests such as individual privacy, commercial interests, and national security.

This paper examines the secrecy statutes passed in the states since the terrorist attacks on September 11, 2001, and concludes these statutes as written do not incorporate safeguards helping to ensure secrecy is the exception, not the rule. This paper suggests criteria for creating openness-based secrecy laws that create appropriate and necessary limits on secrecy. Put another way, the laws developed since 9/11 by the states do not define adequately the boundary beyond which secrecy is *no longer* an appropriate technique for government to use when working to advance such interests as public health, public safety and national security.

Openness and Secrecy Since 9/11

A factor complicating the debate about openness and secrecy in government is that many observers frame this question as a balance between security and openness.[4] This balance test is a straw man

1 The author may be contacted by phone at (703) 807-2100, via mail at 1101 Wilson Blvd, Suite 1100, Arlington, VA 22209 or via email at rblum@sunshineingovernment.org.

2 Affiliation for identification purposes only. All views expressed in this article are those of the author and do not necessarily represent the views of the Sunshine in Government Initiative or its member organizations. The author retains fully responsibility for the contents.

3 House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, , S. Rep. No. 107-351 & H. Rep. No. 107-792, Dec. 2002 (July 24, 2003), p. xix.

4 *See*, for example, Charles M. Vest, *Response and Responsibility: Balancing Security and Openness in Research and Education*, available at http://web.mit.edu/president/communications/rpt01-02.pdf (last viewed November 2, 2007); *Balancing Scientific Openness and National Security Controls at the Nation's Nuclear Weapons Laboratories*, Committee on Balancing Scientific Openness and National Security, National Academic of Sciences, Institutes of Medicine, National Academy Press (Washington, DC) (1999).

for at least two reasons. First, security, just like freedom, is an end in and of itself. Secrecy and openness are tools our government uses to achieve societal goals of freedom and security. By mixing a means (openness) with an objective (security) we are comparing two things that cannot be compared. Second, discussing a balance between security and openness assumes that the relationship is zero-sum, that one is the antithesis of the other. The framing of the policy discussion in this way therefore pushes into irrelevancy the practical ways that openness contributes to the national security, public safety and public health.

At the same time, the debate about secrecy and openness has tremendous salience and resonance since 9/11. Scientific researchers have faced the post-9/11 tension between information sharing and secrecy. In 2004, the National Science Advisory Board for Biosecurity was established to

> provide advice, guidance, and leadership regarding biosecurity oversight of dual-use research, defined as biological research with legitimate scientific purpose that may be misused to pose a biologic threat to public health and/or national security.[5]

In 2005, two researchers sought to publish a paper in a respected scientific journal demonstrating how easily a terrorist could contaminate the nation's milk supply and advocating additional research and early, cost-effective testing to mitigate the threat.[6] The Department of Health and Human Services intervened and requested the article not be published.[7] After a brief review, the editors decided to publish the paper.

In difficult areas of dual-use scientific research, in which a technology or scientific breakthrough can help us and be used against us, is it possible to better define and articulate the line between secrecy and the free flow of information? Recently, the National Academies has encouraged more active communication on the relationship between national security and biological research.[8] Or, is this a disagreement based on fundamental philosophical difference in views on how our government and society handles information? Answers to these questions will have profound impact on our strategies for protecting public health, national security, scientific research and openness in our democracy.

Secrecy Proposals at the Federal Level Are Overbroad

From experience reading proposals floated in Congress and examining the collection of state laws compiled for this conference, this much is clear: legislation passed in the states and in Congress reflects decision makers' ambivalence about when secrecy is the best strategy and when disclosure is preferable to maximize public health and safety. At the very least, lawmakers have trouble clearly writing the difference into law.

At the federal level, Congress continues to write new exemptions into federal law that go beyond the existing exemptions written into the federal Freedom of Information Act (FOIA).[9] The federal FOIA law already has nine exemptions allowing federal agencies to withhold documents, including protections for classified information, trade secrets and individual privacy.[10] In addition, in

5 Charter of the National Science Advisory Board for Biosecurity, U.S. Department of Health and Human Services, Mar. 4, 2004.

6 Lawrence M. Wein, & Yifan Liu, *Analyzing a Bioterror Attack on the Food Supply: The Case of Botulinum Toxin in Milk*, *PNAS* 102:28, July 12, 2005, p. 9984-9989.

7 *Feds: Science Paper a Terrorist's Road Map*, CNN, June 5, 2005, available at http://www.cnn.com/2005/US/06/06/milk.terror/index.html (last viewed 6/7/2005).

8 *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities*, Committee on a New Government-University Partnership for Science and Security, National Research Council, 2007.

9 5 U.S.C. § 552.

10 *See* 5 U.S.C. § 552; "Freedom of Information Act Guide," U.S. Department of Justice, Mar. 2007, available at http://www.usdoj.gov/oip/foia_guide07.htm (last viewed

2006, federal agencies cited 149 separate laws on the books that put information held by the federal government beyond FOIA's reach.[11]

Today, attempting to exempt information from the federal FOIA is routine. Earlier this fall, the Sunshine in Government Initiative (SGI) identified at least 27 bills in the U.S. Congress this year that proposed exempting certain information from FOIA. For two consecutive years, the Department of Defense proposed exempting certain information concerning weapons of mass destruction from FOIA's long reach. This may sound like a reasonable approach, given the threat of terrorism and the possibility of mass civilian casualties if such a weapon were used. The problem, however, has been in the broad construction of the proposal. The Defense Department proposed exempting information from public disclosure any information "concerning" weapons of mass destruction. As SGI noted at the time, this scope is so broad it could include information about vulnerabilities, accidents and safety problems at chemical plants and other challenges to the safety and health of a community's residents.[12]

This is but one experience that raises fundamental questions about laws that allow the government to withhold information from the public. How do we maximize the openness in our society while recognizing the government's legitimate need to keep secrets? How do we better identify when secrecy is the most effective tools for security? Conversely, how do we identify when openness best serves the interests of the public?

Principles for Legislating Secrecy as an Exception

Working in collaboration with the Coalition of Journalists for Open Government, the Sunshine in Government Initiative developed criteria for assessing whether secrecy laws are adequately bounded. They have been adapted for use in the context of both federal and state laws. These principles can serve as a checklist for evaluating new proposals to withhold documents held by the government and, more importantly, infusing those rare secrets with necessary limitations. To adequately limit the impact of secrecy on the ability of the public to stay informed of government's activities, any new exemptions to public records laws should:

1. **Avoid duplication**. Those who propose new secrecy laws should provide a clear statement of public purpose and explanation as to why existing laws are not adequate. Anyone who would propose changes to law might discover upon close examination of existing law that the concerns are not founded and that existing law is adequate. A careful analysis and understanding of what can be withheld from the public under existing law would likely cut down on policy debates about duplicative new proposals, allowing all participants more time to focus on the more difficult, complex situations.

2. **Be surgical.** Laws should be narrowly drafted so as not to exceed the specific non-disclosure needs compelling the exemption. Where broad disclosure is vital to advancing public understanding, any necessary exceptions to disclosure should be narrowly drafted. In areas where free flows of information advance public health, any sensitive information that must be withheld must be clearly identified to allow the maximum benefit from disclosure while

Sept. 26, 2007).

11 *Summary of Annual FOIA Reports for Fiscal Year 2006*, FOIA Post, U.S. Department of Justice, Sept. 14, 2007, available at http://www.usdoj.gov/oip/foiapost/2007foiapost11.htm (last viewed Sept. 26, 2007).

12 *Hazardous Secrecy Proposal Re-emerges*, Sunshine in Government Initiative, May 3, 2007, available at http://www.sunshineingovernment.org/foia/SGI%20on%20WMD%20proposal.pdf (last viewed Sept. 26, 2007).

protecting information the disclosure of which may do harm. Information useful in mounting biological, radiological and chemical attacks on the U.S. population can also be useful in spurring medical advances against disease and illness, so that information to be protected should be narrowly described.

3. **Be accountable.** Laws should provide for public reporting that measures the efficacy of the exemption in achieving its stated goals and that offers alternative and equivalent means of public oversight. Use of secrecy as a tool should be better monitored for at least two reasons. First, when a law is enacted giving the government power to collect information from the private sector and keep it confidential, the public deserves to know whether this closed system is achieving the practical objectives for which secrecy is granted.

   Second, better oversight will strengthen public trust in government by helping ensure government officials are not invoking secrecy solely to avoid revealing embarrassing or inconvenient truths.

   Is the federal government better able to protect critical infrastructure because it can keep information secret when companies volunteer it? Are readers better protected from accidents or possible attacks on a chemical plant in exchange for remaining ignorant of the problems, possible protective measures, and ways to fix them?

   These are not theoretical questions, nor do they call for values-based answers. Rather, for the presumption of openness to have meaning, secrecy should be acceptable only when traded for identifiable and wherever possible measurable benefits to the public.

4. **Include sunsets.** Laws should establish a time limit after which the exemption expires and requires affirmative action to renew. Also establish a built-in sunset provision for the entire statute or for that section of statute which establishes the b3 exemption. Were it to develop a vaccine against anthrax, the government may seek to withhold details about specific ways to disarm that vaccine. If such secrecy were granted, it would be in the face of an acute threat for a limited amount of time until the known threat is eliminated or the disarming technique is known. Such secrecy should be publicly reviewed (preferably by a party with no interest in the relevant government activity) to assess whether continued secrecy is warranted. Affirmative action should be required for the government to continue its withholding.

5. **Protect whistleblowing.** Laws should make clear that the non-disclosure provisions, along with any penalties established to enforce them, are not intended to inhibit whistleblowing. Non-disclosure agreements should not protect wrongdoing such as waste, fraud and abuse or illegal activities.

6. **Allow public review.** Any legislation proposing exemptions to public records, public meetings or other open government laws should be publicly identified and reviewed for their impact on openness.[13] Congress could refer all bills (or their relevant sections) that contain a FOIA exemption to the House and Senate committees with jurisdiction over the FOIA for review by staff with experience with FOIA laws. Just as they summarize privacy or budgetary

13 Because it is a matter of the legislative process which would not be readily apparent from an analysis of the legislative text of statutes passed since 9/11, this element was not included in the analysis of the state statutes that follows.

impacts of bills approved in committee, the House and Senate could adopt rules requiring committees to conduct openness impact statements. State legislatures could adopt similar approaches.

7. **Balance incentives.** Laws should impose no penalties for release of information greater than those provided by law for improper withholding of information. Penalties, both perceived and actual, for improperly disclosing sensitive information far outweigh the penalties associated with improperly withholding documents. Legislators should develop additional tools to create consequences—both positive and negative—for improperly withholding documents from the public.

A Brief Note on Methodology

For this analysis, we used a content analysis of the legislative language itself to evaluate whether each bill text met the seven criteria.

Caveats. The author of this study did not review other material, such as news coverage, legislative history or outside analyses. An inherent limitation of primarily examining bill texts is this analysis did not identify earlier drafts of the legislation, amendments and other modifications made during the legislative process, additional views on the bills, or the motivations of those political actors (i.e., legislators, state officials, interest groups) involved in the policy debate. This additional knowledge could affect the analyst's ability to predict the impact of the legislation on the public's availability of information about public health issues.

It should also be noted that relevant qualifiers affecting the breadth of the secrecy required or allowed in each law passed since 9/11 may not appear in the provision of law but may exist elsewhere in the statute. A withholding statute may be part of a broader statute subject to a sunset date.

New statutes requiring or permitting agencies to withhold documents may also suffer unintended consequences. To the extent that statutes asserting that information should be protected could be perceived to conflict with whistleblower protections elsewhere in the law, new laws preventing disclosures should include a statement reaffirming the rights of whistleblowers already in law.

Analysis: Applying the Principles

To evaluate whether secrecy provisions are bounded so as to preserve the presumption of openness, thirty-one statutes were examined from the research compiled for this conference. Several statutes that appeared to provide for withholding were excluded because the extent of the withholding could not be determined from the provided text.

As the table in Appendix A shows, the principles outlined above did a relative poor job of differentiating one statute—or one state's performance—from another. State legislatures shielded categories of information based on subject matter or type of document without providing wholesale discretion to withhold documents. Beyond that, however, these strategies for limiting information—creating time limits, creating statutory requirements for review accompanying new secrecy provisions, clarifying how secrecy provisions relate to other requirements such as whistleblower protections—were clearly and absent from state secrecy statutes enacted in recent years.

Topics/need statement. Of the selected statutes, all clearly defined a topic or subject area. None provided blanket discretion for a state agency to withhold records. Many laws, however, left to agency judgment whether disclosure would assist terrorist attacks without providing criteria or a method for calculating the risk.

Most of the public health statutes focused on protecting physical infrastructure necessary to maintain human life—buildings, water supply

systems, energy infrastructure. Surprisingly few statutes dealt with the most interesting of public health questions: how information about new scientific discoveries is handled. Here the possible approaches—secrecy or sharing—are the starkest and the pitfalls the greatest. At what point is secrecy about the workings of a new vaccine—or the vaccine's own vulnerabilities—justified to protect this country's ability to protect public health? Once granted, how is secrecy reviewed and overturned once knowledge has been shared broadly and its secrecy no longer relevant? And who decides? Experts with sufficient knowledge of and independence from the government activity? Those people in government who also have a keen professional interest in the success of the program? Or legislators, who may address these questions on an ad hoc basis writing new laws, often the least discriminating of policy tools?

Narrow construction. Comparing the laws authorizing the withholding of information from the public, three interesting lessons are yielded. First, states broadly were concerned with withholding information out of a concern that it may be useful to terrorists, such as critical infrastructure emergency response; providing protections. Second, state laws reflected a concern after 9/11 that those protections be sufficiently broad to provide clear protections. Only a few states affirmatively noted types of related information that should remain public. Third, states responded to the threats made real by 9/11 by requiring new reports and information to be shared within government and putting that information largely beyond the public's grasp.

Critical infrastructure. The language in most statutes gave broad coverage to specific types of information. Many state legislatures since 9/11 wrote laws keeping from disclosure an information the government holds about safety problems or vulnerabilities with complex systems supporting energy transmission, water supply, food distribution and transportation network. Protecting such networks has become such a policy imperative since 9/11 that a new term describing them has entered the policy lexicon—"critical infrastructure." North Dakota defined the term broadly to include any system whose destruction would have a "debilitating impact" on the economy, security or public health or safety of the state. The state government in North Dakota can withhold plans for protecting critical infrastructure throughout the state, including government as well as non-government.

Emergency response. Many state laws passed since 9/11 reflected concern about what would be known either to terrorists or the public generally about government plans to respond to terrorist attacks. West Virginia exempted from disclosure records "assembled, prepared or maintained" about government activities before, during or after a terrorist attack. Other states did the same. Nevada can avoid public inspection of its comprehensive response plan, although officials may decide to disclose information during an emergency. Maryland arguably established the most limits on the state government's ability to withhold its terrorism response plans. Government officials can deny requests to review emergency response documents if disclosure would assist terrorist attacks or endanger public health. Government buildings are exempt from such withholding, and the statute clearly states that routine inspections are public and details about buildings involved in fires or other catastrophic events are public. In Missouri, officials must find that disclosure will impair its ability to protect public health and safety, and that the public interest in withholding outweighs the benefits of disclosure.

Protecting new information collections. In many cases, state governments wanted to collect information and had to promise in new laws that the public would not see it. In New York, companies that produce and deliver energy must report on their security efforts to the State. The reports are largely public but certain documents can be kept confidential. Oklahoma went further, broadly

barring seven state agencies that regulate energy production, including the state's environmental protection agency, from releasing environmental and safety threats existing in the energy industry's infrastructure. Utah protects disclosures of vulnerabilities in the food supply.

Several states were concerned about the condition of the public health system. Ohio now requires trauma centers to report on their preparedness to a public health council. Even the council's guidelines for reporting are confidential, although a summary is public. In Nevada, hotels and resorts must develop comprehensive response plans, but those are not public.

Sunsets. The statutes, with rare exceptions, also share a failure to establish a time limit for the secrecy. Such time limits can come in at least two forms: sunsets on the authority to withhold and secrecy expiration dates.

Sunsets on the authority to withhold
Legislatures can sunset the authority to withhold documents. Legislatures can at a future date renew or extend that authority, hopefully after assessing whether the secrecy has created any public benefit. However, without a provision to automatically sunset the government's authority to withhold information, legislators are unlikely to review or reverse new laws granting the power to withhold. State legislatures were unlikely to limit the time information could be withheld. In Arkansas, the state legislature allowed the state to broadly keep secret virtually any information about vulnerabilities or safety problems of water systems if disclosure might jeopardize or compromise efforts to protect the water system.

Secrecy expiration dates
In addition, the time limits can apply to the withholding of specific information. For example, in the federal government when a government official creates a document that needs to be classified, the official designates when the information can be declassified. This analysis could not find any state law that used this limitation.

Other Measures: Whistleblowers & Penalties. The statutes universally did not include whistleblower statements or address penalties for improper disclosing or withholding.

The Benefits of Openness: A Research Agenda

In the late 1990s, the Environmental Protection Agency dipped its toes into the waters of assessing the benefits of openness. The federal agency had been discussing its plans, mandated by the Clean Air Act Amendments of 1990, to compile industry-written emergency response plans based on estimates of the impact in surrounding communities of worst-case scenarios at thousands of chemical plants around the U.S. The EPA planned to make these available on the Internet in searchable form and distribute CD-ROMs with the database available to anyone who requested it. Some representatives of plant operators argued that public availability would substantially increase risks of terrorist attacks. The debate elevated. Congress got involved and within days of this data being available to the public, Congress exempted this information from the federal Freedom of Information Act for one year while EPA and the Justice Department conduct separate assessments of the benefits and risks, respectively, of public disclosure.[14]

That EPA benefits assessment consisted of case studies and anecdotes and concluded that there were, in fact, benefits to public disclosure, especially as it related to public safety. This 149-page document is perhaps the most ambitious effort to pull together wide-ranging case examples of the practical public health benefits of disclosure of government held information.[15]

14 Chemical Safety Information, Site Security and Fuels Regulatory Relief Act, Pub. L. 106-40 (enacted Aug. 5, 1999).

15 U.S. Environmental Protection Agency, *Assessment of the Incentives Created by the Public Disclosure of*

Moving one step in this direction, the Sunshine in Government Initiative (SGI), the coalition of media groups for whom I work, has catalogued approximately 250 stories of value to the public—mostly from media outlets but including advocacy groups and researchers—that relied upon access to documents under the federal FOIA.[16] We have catalogued these stories and summarized their contribution to the public's understanding of issues from veterans' benefits to education and made this collection available online at our website, *www.sunshineingovernment.org*. Our objective is to provide a resource for anyone who wants to know or demonstrate how FOIA is used by the news media or anyone else to inform the public and the practical benefits of our open government laws.

SGI's *The FOIA Files* is only a first step. Unfortunately, we do not yet have a collection of similar stories and their impact that relied on state openness laws. We hope in the future someone will collect that information. And in focusing on the Freedom of Information Act, this database does not address how society benefits in practical ways from government agencies *proactively* posting information on websites and making databases of information available to the public. So this is a limited but, we hope, significant step to helping the public and decision makers see the practical as well as philosophical value of openness.

3.2 Model Citizenship in the Management of Public Health Emergencies – The Role of Open Government

by Monica Schoch-Spana, PhD

Abstract

Improvements in the nation's ability to handle both emergent and familiar health threats depend upon deliberate planning for the smart flow of information among officials and with the public. The new field of public health preparedness has been predisposed towards a "closed" system in which political leaders and their health, safety, and security advisors—at all levels of government—have defined the direction of health emergency management policies and plans without sufficient input from the populations that they seek to protect. Under these conditions, the citizen role in helping remedy health disasters has been very circumscribed, leaving undeveloped any broad understanding of, or institutionalized mechanisms for tapping the valuable contributions of citizens and civil society throughout the complete disaster cycle. To help remedy this deficit, this paper describes and illustrates a continuum of public-spirited contributions that civic groups and individuals can make to health emergency management, and it calls for a model program that would establish and sustain "community engagement" as the national standard for state and local health emergency planning.

Introduction

This paper reviews factors that have predisposed the emerging field of "public health preparedness" towards a closed system in which political leaders and their health, safety, and security advisors—at all levels of government—have defined the direction of health emergency management policies and plans without sufficient input from the populations that they seek to protect.[17] Under these conditions, the citizen role in helping remedy extreme health events has been very circumscribed, leaving undeveloped any broad understanding of, or institutionalized mechanisms for, tapping the

Off-site Consequence Analysis Information for Reduction in the Risk of Accidental Releases, Apr. 18, 2000; *See also*, U.S. Department of Justice, *Assessment of the Increased Risk of Terrorism or other Criminal Activity Associated with Posting Off-site Consequence Analysis Information on the Internet*, Apr. 18, 2000.

16 *The FOIA Files* is available through the website of the Sunshine in Government Initiative at http://www.sunshineingovernment.org.

17 This paper re-examines, in terms of an "open government" framework, earlier concepts, arguments, and recommendations developed by the author and associates elsewhere (*e.g.*, 23, 52, 54-56, 69).

valuable contributions of citizens and civil society during the complete disaster cycle.

To help remedy this deficit, the paper describes and illustrates a continuum of public-spirited contributions that civic groups and individuals can make to comprehensive health emergency management, and it calls for a model program that would establish and sustain "community engagement" as the national standard for state and local health emergency planning. The civic infrastructure—the public's collective wisdom and ability to solve problems; voluntary associations that arise from shared interests or a public good, and that meet on-line or face-to-face; and non-profits that protect the well-being of various groups—is essential to managing a mass health emergency. Community engagement is the practical means by which officials can access that dynamic whole.

Before turning to how leaders, in and out of government, may wish to redefine citizens' role in health emergency management, the paper provides a quick overview of other public health debates in relation to information-sharing policies and practices after the 9/11 attacks and the anthrax letter deaths of 2001. This review is meant to alert the reader interested in "open government" to the large biodefense universe, illustrating the range of transparency debates and discussions within. This survey and the larger argument to follow show that future improvements to the nation's ability to handle emergent and familiar health threats require deliberate designs for the smart flow of information among officials and with the public.

Public Health Impacts of Biodefense Information Sharing Policies

Various authorities during the 1990s expressed mounting concern about re-/emerging infectious diseases, terrorists' interest in mass casualties, and the increased availability of unconventional arms such as biological, chemical, and nuclear weapons (32, 62). Events in the fall of 2001 consummated their worst fears about dangers facing the country in a world no longer defined in terms of a nuclear stand-off with the Soviet Union. A trickle of federal investments prior to 9/11 burst into an immense funding stream and plethora of initiatives to protect civilians against biological attacks—over $34 billion in FY2001-2007 (20). Two top priorities are improving the biomedical research infrastructure to produce vaccines, antibiotics, and diagnostics against potential threats and enhancing the ability of the medical and public infrastructure to contain the effects of a bioattack and help survivors.

Many government transparency issues have arisen in the pursuit of these objectives (e.g., 24, 26, 31, 67). The select cases below involve potential adverse health effects in connection with how information is generated, collected, analyzed, verified, communicated, and acted upon. They also represent the 3 traditions in open government depicted by Fung *et. al.* (2007). Preparedness spending presents a classic right-to-know situation in which transparency can help rule out the arbitrary use of government funds and confirm their intended outcome as genuinely protecting the public's health. Safety data and their use in regulating the growing numbers of biodefense research labs illustrate an opportunity for "targeted transparency" in which public access to technical data helps remedy a specific risk or public service failure. Community engagement in emergency planning, addressed later, is part of a third generation in transparency policy in which the public collaborates with officials in producing the very knowledge that can reduce risk and enhance safety.

Fiscal Accountability and Public Health Preparedness

Diverse analysts have noted that systematic understanding is lacking about the effects of the recent, immense federal investments in basic public health infrastructure (e.g. 27, 30, 31, 39, 52, 67). Federal spending on state and local preparedness began at moderate levels in 1999 ($40M) and 2000

($50M), but then jumped 20 fold after the 9/11 and anthrax letter attacks of 2001 and has continued at this magnitude ever since (70). Beginning in FY 2001 and including estimates for FY2007 and FY2008, the federal government will have spent roughly $9.1 billion dollars on agreements with state and local health agencies and hospitals to improve public health capabilities and bioterrorism preparedness (20).

Two nagging questions dominate discussions about these expenditures: Have they, as intended, improved public health preparedness within state and municipal jurisdictions, and the nation as a whole? Have they unintentionally reduced localities' focus upon more familiar population health needs such as water quality, routine immunization, and maternal and child health? (27, 31, 52, 61) Among factors fueling these uncertainties is a lack of agreement among health agencies and professionals about the best way to measure, verify, and communicate to federal funders and the public about improvements in preparedness capabilities and outstanding vulnerabilities (27, 31, 39, 67). Another major cause for ambiguity is the absence of any objective mechanism to track how states allocate and account for federal preparedness dollars (27, 31, 52, 67).

Anecdotal evidence suggests that some health agencies were unable to secure additional qualified personnel and resorted to transferring staff from other divisions to fill the new preparedness positions (27, 31). Reasons given for this include hiring "freezes," desire to retain staff who had lost other grants, lack of competitive salaries to attract good candidates, and limited faith in the constancy of federal support for the new job slots (27). The appearance that many localities have supplanted public health budget cuts with federal biodefense monies led Congress to require in the *Pandemic and All Hazards Preparedness Act of 2006,* that states provide a portion of matching funds for preparedness programs and also undergo an independent audit.

Biosafety Concerns with the Rapid Growth in Biodefense Laboratories

The number of laboratories and investigators researching risky biological agents has grown exponentially since the 2001 anthrax letter deaths, eliciting concerns among industry observers and host communities about potential harm to workers, the public, and U.S. reputation abroad (26, 28, 44, 50). Having identified biological weapons and use by terrorists as possible security threats, the federal government has invested heavily in the research, development, production, and procurement of "medical countermeasures" such as vaccines, antibiotics, and diagnostic tools for biological agents of greatest concern such as smallpox, anthrax, plague, and ebola. From FY2001 through FY2007, almost $17B in federal funds have spent (or appropriated) for bioweapons-related research and development, and approximately 10% of this amount has been reserved for the construction of new high containment research facilities (44).

The burgeoning infrastructure dedicated to infectious diseases research has raised questions about the very scale of the effort, especially given the rapid increase in lab space where the most contagious of lethal agents are handled (BSL-4, BSL-3). Before the terrorist attacks of 2001, only 5 BSL-4 laboratories, which handle the most dangerous agents, were in operation; now they number 15, including at least one in the design stage (50), and even more are anticipated (26). The BSL-3 lab total is less certain, because no single federal agency has the responsibility to track the growth now occurring across federal, state, academic, and private sectors (50). One DHS and HHS estimate from 2005 puts the number of BSL-3 labs in the U.S. at over 600 (26).

Some observers have noted the absence of a rational strategy for the vast expansion; this omission along with a lack of transparency about lab policies and research directions may undermine international confidence in U.S. commitments to global

biosecurity and the Biological Weapons Convention (28, 44). Many researchers and technicians filling the new facilities are novices in high containment research, and the influx will likely strain the current system of biosafety training, according to industry experts (26). Moreover, no objective and transparent mechanism for the tracking and analyzing of accident reports and near misses exists to improve safety practice and performance; certain government rules impede labs from sharing lessons learned with one another (26, 28, 44).

The dramatic scale-up in high containment research, analysts note, increases the chances for biosafety errors and for criminal access to controlled pathogens (26, 28, 44). Public protests have arisen in many locales where new containment research is planned, due in part to highly publicized laboratory mistakes such as tularemia infections in lab workers at Boston University and the discovery that Texas A&M University failed to report lab-acquired infections to the Centers for Disease Control and Prevention (26). Biosafety oversight and regulation has yet to keep pace with the tremendous growth in research with dangerous pathogens, and processes for keeping host communities informed about siting decisions and operations are poorly developed (26, 28, 44).

Pursuit of increased safety in the context of bioattacks and other health emergencies may inadvertently compromise the public's health, although it does not have to. Potential effects include a reduction in routine public health services or insufficient development in health agencies and hospitals' ability to handle extreme health events—the result of unknown outcomes and expenditures. Others are unacceptable biosafety incidents or harms to U.S. international standing—possible costs of intensified scientific understanding of pathogens and potential countermeasures. The next sections consider a third question about "net" health gains with the institutionalization of biodefense: Do local health emergency systems have all the relevant information and public support necessary to achieve intended goals? In each of these 3 cases—budgets, labs, and local planning—intelligent open government can help overcome uncertainties concerning societal investments in biosecurity and inform future policy developments.

Public Health Emergency Management as a "Closed" System

Health authorities and the public they hope to protect may have contended with epidemics and mass casualty disasters before, but the field of public health preparedness—as a self-conscious collection of concepts, practices, and organizational forms—is still very young. Certain aspects of recent history have predisposed the discipline towards a closed form of governance. That is, a societal enterprise with limited input from broader publics, those outside the circles of political and technical authorities now deciding courses for action in the context of emergent health threats. Factors contributing to this trend are assumptions about how the public behaves in disasters and epidemics, the impact of federal programming on state policy and practice, and a broader shift toward enhanced secrecy as a function of national security concerns about terrorists.

The 'Panicky Public' as Foil to Professional Planners & Responders

Prior to 2001 when catastrophic terrorism and biological incidents were serious but postulated dangers, U.S. officials frequently conceived public reactions to a biological event as part and parcel of the crisis: the "worried well" who would pour into hospitals and hinder health care workers' ability to treat "real" victims. The perpetrator, the pathogen, and the public were all forces that seemed to demand containment by authorities (56). Playing one-dimensional roles in hypothetical scenarios and tabletop exercises, members of the public usually surfaced as mass casualties or hysteria-driven mobs that would self-evacuate affected areas or resort to violence to gain access to

scarce, potentially life saving antibiotics and vaccines (57).

Such typecasting arguably was seen as necessary to prepare planners and responders for the "worst case," and to devise contingency plans for managing the public so that the professionals could perform their respective missions. In contrast, extensive social research into disasters, terrorist attacks, and even epidemics of novel disease, reveals that people rarely fall apart and put themselves first (11, 13, 23, 35, 41, 48, 59). This finding contradicts what people tend to say on surveys that ask them how they *think* they will behave when disaster hits (63). Panic is the exception and ordinary people emerge as innovative problem-solvers who are responsive to the needs of others around them. The overriding notion of the "problem public" to be managed precludes careful consideration of, and planning for ways to solicit the cooperation of affected populations. Emphasis instead is on crowd control, not enhancing people's ability to cope with a public health emergency.

Civil Defense, Emergency Management, and Community Partnerships

The notion of the public in the context of a biological attack as, at best, getting in the way of the professionals, and at worst, constituting a secondary disaster, is in keeping with much of the thinking within the history of North American civil defense and emergency management as quasi-military activities. Disaster planning, by and large has been seen as something done *for*, not *with* the community (38, 43, 73). The organizational emphasis, instead, has been on a chain of command among authorized personnel and on centralized decision-making and communications (17, 73).

Certain events have chipped away at this model of insular authority. The 1984 Bhopal tragedy helped spur a series of right-to-know laws and regulations that enabled local people to learn more about the chemical hazards in their communities and improve plans for responding to a major chemical accident (7, 22, 38, 40, 51). The Local Emergency Planning Committees (LEPCs), mandated by SARA Title III, consciously called for a diverse set of stakeholders to sit at the planning table including public safety officers, planners, health care providers, environmental specialists, industry representatives, school representatives, journalists, and environmental and community action groups (7, 38, 40).

In the 1990s, facing an escalation in the economic and social costs due to natural disasters, FEMA began a national effort to shift the focus of state and local jurisdictions toward *pre*-disaster activities that could reduce risks and cut the costs of post-disaster recovery (4, 66, 71). Among the new programs stressing hazard mitigation was "Project Impact," whose core objectives included reaching constituencies outside the traditional emergency management profession and building up new partnerships among local government agencies, nonprofit organizations, and private businesses (4, 71). Both the LEPCs and Project Impact (prior to being defunded in 2000) have had mixed success at involving local civic groups, and in particular, those who represent vulnerable or marginalized populations (38, 40, 71). Yet, overall these grassroots initiatives do signal a more inclusive, transparent approach to emergency management.

Terrorism, National Security, & Renewed Emphasis on Secrecy

Whereas disaster-related events in the 1980s and 1990s helped advance the turn toward community right-to-know and partnerships for comprehensive disaster management, government responses to the 9/11 attacks have provoked a different set of trends, as a number of disaster, public health, and legal scholars have noted in greater detail elsewhere (6, 7, 10, 25, 29, 54, 66, 72, 73).

Concerns about future terrorist attacks threats spurred many federal agencies to remove publicly

accessible information that revealed potential vulnerabilities within the U.S. critical infrastructure (6, 7, 10, 25, 54). The perceived tension between environmental health and national security objectives continues with different levels of government trying to find the right balance between legitimate security concerns and a community's right to know (6, 10, 54). The reasoning in the case of chemical facility data, for example, is that the same information that alerts the public to potential toxic releases within their communities may also provide terrorists an advantage in selecting and attacking targets (10, 54).

Prior to 9/11, disaster management was the purview of a new class of professional emergency managers who—driven by events in the 1980's and 1990's—had come to embrace a model of integrated emergency management (29, 66, 73). Elements of this conceptual framework included an "all-hazards" perspective that seeks to create flexible institutions that can deal with the most frequent, geographically specific hazards in a community and also be able to address a range of unforeseen extreme events (66). Integrated emergency also incorporates the classic four phase disaster cycle that sees the protective interventions of mitigation, preparedness, response, and recovery as part of a single, iterative process (66).

In contrast, the rising field of homeland security, due to its counter-terrorist priorities, has come to be populated by law enforcement and military-trained professionals whose organizational culture incorporates the top down, command-and-control approach characterizing an earlier generation of civil defense (29, 66, 73)—the one from which emergency managers had been turning away to embrace a model of shared responsibility among community partners (38). Homeland security also has a core posture of readiness to act swiftly when a terrorist attack occurs. The focus on picking up the pieces after the fact, however, has eclipsed the longer term perspective necessary for both pre-disaster loss reduction activities and post-disaster reconstruction and recovery (66). Moreover, the value placed on countering terrorism has overshadowed an "all hazards" mindset. Some analysts attribute this shift as a partial contributor to the failed governmental response to Hurricane Katrina (66).

Federal Investments in Preparedness & the Turn to 'Risk Communication'

As noted earlier, public health preparedness was a field inclined, in the early imaginations of planners and responders, to see the public as either passive victims or active rioters (55-57). Once the 9/11 attacks occurred, the field continued to evolve in the context of a larger political and organizational milieu stressing limits to public information as a function of national security—the USA Freedom Corps and *ready.gov* notwithstanding as developments to involve the public in homeland security.

Some public health and civil rights advocates also worried about the new collaborations necessarily emerging between law enforcement and public health practitioners (3, 24, 34, 61). A biological attack would trigger two very different kinds of critical investigations: one to identify and neutralize the attacker; the other to identify victims, contain the disease, and provide medical care. How security and health officers might effectively work together to achieve their respective aims was uncertain. Would counter-terrorism aims overshadow those of protecting the public's health? (24, 61) Would confidential health data be put to use by law enforcement, and if so, what did that mean for public privacy and the public trust that health professionals need to do their work? (24, 34) Would people avoid seeking medical attention if they felt their personal health information might somehow be used against them? (3, 24, 34)

The new patterns of information sharing practices in the aftermath of 9/11 provoked these and other questions among health professionals who now had to contemplate the prospect of biological at-

tacks in addition to more familiar health threats. The complex realities of the 9/11 attacks and anthrax mail crises did refine, however, many authorities' understanding of the public not simply as a problem to be managed, but a constituency to be served: anxious people understandably in need of good information about what the danger was and what to do about it. Communications failures on the part of authorities spurred recognition of how public outreach is part of managing the effects of a bioattack. Missteps included public officials' underestimation of the significance of the first anthrax death and an over-reassurance of the public, public health authorities' lack of clear medical "next steps" in the midst of an urgent population health matter, and the perceived unequal treatment of exposed Capitol Hill and postal workforces (23, 49, 64).

Following the anthrax crisis, U.S. federal health authorities thus identified "risk communication and health information dissemination" as 1 of 7 priority areas in their guidance and financial support to upgrade the ability of state and local health departments to respond to bioterrorism (discussed above). Critical reflection on responses to the 2001 attacks also spurred the release of many helpful analyses and guidebooks for officials regarding successful communications with the media and the larger public (8, 19, 69). Prevailing approaches among decision-makers and professional responders toward the public have now shifted in great measure from an earlier emphasis on containing disorder to communicating information to citizens in a public health emergency. The communication model is reminiscent, however, of command-and-control organizational forms where warning messages are seen to emanate from a center outward. Citizens are expected to remain alert to uncertain and evolving events, awaiting instructions about what to do from officials who are adept at risk communication (55).

The People's Role in the Life Cycle of a Major Health Emergency

In the context of a closed preparedness system, the perceived citizen role in health emergency management is very circumscribed. Individualized activity has been the object of official interest and intervention, more so than collective endeavors. Household readiness is the concept most prevalent in popular culture (if not in practice), followed by volunteering and direct problem-solving by nonprofits. Notably absent are structured and sustained opportunities for public deliberation and input about preparedness policy, implementation, and outcomes.

Self-Reliance, Personal Stockpiles, and Ready Households

U.S. residents are on the receiving end of much thoughtful advice about individual and household preparedness for a variety of hazards (2, 14, 16, 68). In this self-reliant approach, members of the public ready themselves by preparing contingency plans for their families, including a strategy to keep each other informed of personal location and well-being. Officials also consider it prudent for members of the public to stockpile enough food, water, and other essentials to be self-sufficient until help arrives or the crisis resolves—72 hours being the general rule of thumb. Another recommended act of self-sufficiency is becoming familiar with the special challenges posed by unconventional terrorist attacks that involve chemical, radiological, nuclear or biological agents.

Reasonable arguments support the notion of a public equipped to make do on its own. Self-study of unconventional attacks may reduce the shock value of otherwise novel and insidious hazards such as radiological, chemical and biological weapons. Family plans for emergencies target a prac-

tical and meaningful solution to one of the most emotionally wrenching qualities of an extreme event—worry and uncertainty about the welfare of loved ones. Compiling an emergency kit that includes flashlight, radio, fresh batteries, non-perishable foods, maintenance medications, and other "basics" is a do-able, human-scaled project that—depending upon the circumstances—can have real material value, and also brings intangibles like personal safety and security into being. Lastly, from the perspective of disaster response professionals, every self-sufficient individual and household lightens the burden of having to protect an entire population, focusing limited resources on the most needy.

Family communication plans, emergency kits, and self-study of threat agents are sensible preparedness activities, but with notable limitations. Capable institutions and professionals—including those that make up the health care and public health systems—are still necessary to handle the needs of large numbers of people. In a bioattack, it certainly helps for private citizens to be informed and alert to specific symptoms, but if doctors and health authorities do not know the next best steps or have not jointly planned community-wide contingency plans, a community's well-being may still be in jeopardy.

Volunteering during the Response & Recovery

The extent to which citizens have acted on this advice, however, is not what disaster planners and educators would hope (37). Some Americans have moved beyond disaster preparedness, however, as a private act like stockpiling to a public good by volunteering their time in a variety of national and local programs. Government sponsored programs include the Citizens Corps and its constituent volunteer programs such as the Medical Reserve Corps and the Community Emergency Response Teams (58). Non-governmental programs include the Red Cross and Voluntary Organizations Active in Disaster (a collection of social service organizations who have agreed to perform their respective missions as needed in disaster settings).

Community-oriented groups are also acting on behalf of the public good for disasters. The National Organization on Disability, the American Association for Retired Persons, and the Red Cross recently joined the DHS in preparing brochures that provide seniors and disabled persons preparedness tips directly relevant to their circumstances (1). Collaborating Agencies Responding to Disasters (CARD) emerged in the aftermath of the Loma Prieta earthquake and the Oakland Hills firestorm as the publicly-minded mechanism to train, unite, and coordinate Alameda County service providers as a safety net for people with little or no ability to address their own preparedness, response and recovery needs such as seniors, children, the disabled, the homeless, non-English speakers, and low income families (12).

"Disaster-conscious" households and non-profits are significant achievements in terms of civic engagement in a pressing public policy issue. But important gaps remain. First, notions of citizen and community preparedness play an important rhetorical role in homeland security. Yet, their symbolic significance is not matched by a commensurate level of public funding, judging from a proxy index such as the inconsistent and diminishing Citizen Corps budget (58). Secondly, the prevailing emphasis on household stockpiling and individual public service represents only one important point along a much broader continuum of "civic preparedness"—that is, the total of private and public measures that citizens can adopt to mitigate the communitywide problems of disasters and epidemics.

Civic Duties beyond Individual Public Service in the Disaster

Defining the citizen role in a health emergency strictly in terms of ready households and emergency volunteers—both absolutely essential civic

goods—may inadvertently make it easier for people to rescind on another kind of public-spirited obligation: paying closer attention to the politics of disaster. By "politics of disaster," what is meant is the relative value placed on health emergency management amidst other societal problems and policy solutions, as well as the difficult tradeoffs that can arise in relation to specific policies to mitigate, prepare for, respond to, and recover from extreme events (cf. 46).

Complex reasons explain the lack of opportunities and demands for this collective, public-minded aspect of civic preparedness. Elected officials may be reticent to hold public conversations about the psychologically wrenching aspects of large-scale and/or long-duration tragedies, and emergency response and health professionals may hesitate to articulate out loud the limits to their professional tools and institutions to protect entire populations. Often eager to volunteer, Americans are in comparison less practiced with democracy's "pluralistic" and "agonistic" sides (9). Civic engagement scholars note that U.S. has a history of vigorous participation in voluntary associations where members mix with similar others for a common pursuit (47, 60); far less frequent are exchanges on community matters among people with diverse backgrounds and opinions (15, 18, 33, 65).

Whatever the cause for this neglected aspect of civic preparedness, the situation is no longer sustainable. The Gulf Coast tragedies painfully called into question the collective resolve and capacity of Americans, in and out of government, to care adequately for one another in catastrophic circumstances (66). Community engagement, as the next section describes, is one intervention that leaders can take to help evolve all points along the civic preparedness continuum.

Sustainability of Citizen-Aided Remedies for a Public Health Emergency

The civic infrastructure—the public's collective wisdom and ability to solve problems; voluntary associations that arise from shared interests or a public good, and that meet on-line or face-to-face; and non-profits that protect the well-being of various groups—is essential to managing a mass health emergency and other large-scale disasters, yet policy and practice rarely articulate well with this critical resource. Community engagement, a complement to mass communications and ad hoc consultation, is the practical means by which officials can access that dynamic whole. Public participation methods are under-utilized despite indicators from research and practical experience that these tactics, in contrast to mass communications, may help leaders tackle some of the more intractable problems posed by extreme events (53, 59).

How to Tap into the Civic Infrastructure's Talent at Managing Emergencies

The civic infrastructure—rather than the lone citizen, individual household, or undifferentiated masses—provides a very specific target for leaders to incorporate into health disaster policy-making and implementation (59; see Figure 1). In the pre-event period, it can help set policy priorities, inform value-laden policy decisions, and function as a "multi-frequency" communications network that can reach dispersed and diverse populations; during the crisis and recovery periods, it can support responders, tackle unforeseen problems, and identify priorities for rebuilding.

Leaders have a range of techniques through which to mobilize elements of the civic infrastructure in (and for) disasters (53). Operating in a "communication" mode, an official or agency conveys information to members of the public in one-way

fashion, often with the intent of educating and informing the populace. Public feedback is not required or specifically sought out. Alternately, leaders may assume a "consultation" posture, soliciting opinions through surveys, polls, focus groups, and advisory panels. The public's opinions, criticisms, and constructive advice comprise only one factor among others for a policy maker's consideration. In contrast, "engagement," the third approach, constitutes a two-way flow of information between authorities and citizens, where dialogue helps foster a more nuanced understanding of a complex issue, and where the goal is to work together to conceive and implement a policy solution.

In this latter modality, leaders expressly seek out the counsel of citizens and consciously share decision-making power, to more or less degrees, depending upon the context. Citizens, in turn, draw upon and exercise collective power through open deliberations and/or having their interests represented by local opinion leaders working alongside authorities. Ideally, these conversations help them to glean views of a problem that reach beyond their immediate circumstances and to learn how to make appropriate demands upon government (that is, act as a public) and what government may need from them to meet those requests (45). This last and most robust form of public involvement has yet to be incorporated into public health preparedness. It is nonetheless very promising in terms of developing socially acceptable plans to distribute scarce life-saving medical resources and to care for large numbers when the formal health care system is overwhelmed or incapacitated (58-59).

"Civic Preparedness" Continuum for Public Health Emergencies

The citizen role in health emergency management, as largely conceived today, suffers from a complex myopia: the stress upon private citizens acting alone rather than civic groups like faith communities, neighborhood associations, trade organizations, and social clubs pulling together; the weight given to improving individuals' emergency stockpiles and coping skills at the expense of developing more public-minded contributions throughout the disaster cycle; and lastly, the valorization of volunteers' physical contributions during the crisis while their mental and moral problem-solving abilities remain untapped in the planning periods long before and after an event. These deficits in public health preparedness are all the more apparent when one looks at the rich history of citizen-aided remedies for epidemics and disasters (13, 23, 35, 38, 41, 51, 57, 58).

In the case of polio in the mid-20th century, U.S. citizens had their own analog to *ready.gov* and *pandemic.gov* suggestions for individuals to make a kit and have a plan: don't get over-tired, wash your hands, don't catch a chill, allow your children to play with friends but not strangers. Outside the realm of monitored individual behavior, however, regular people made sweeping contributions to the prevention and treatment of this dreaded, highly visual disease that crippled children in the post-war period—a time when infectious disease was thought to have been conquered by miracles like penicillin (41). The March of Dimes facilitated this social crusade, turning philanthropy on its head by seeking small donations from millions of Americans rather than large contributions from a few wealthy individuals and inspiring civic groups to take up roles in mass vaccination (41).

Local chapters organized "mothers' marches on polio" to raise funds through door-to-door neighborhood canvassing, and these donations helped support research and development for both the Salk and Sabin polio vaccines (41). People donated their time and money to help carry out the clinical trial of the Salk vaccine in 2 million children, the positive results of which were received "as if a war had ended" (41). Civic groups, such as the Junior Chamber of Commerce, also volunteered with health departments in a mass vaccination program known as "Sabin on Sunday," a

campaign that reached 80–90% of the target population, a critical step to eliminating polio in the U.S. (58) Today, voluntary groups such as Rotary International are the engine for National Immunization Days around the globe, vaccinating against polio; on a single day, volunteers in Brazil vaccinated nearly all children under five years old against polio (58).

Such dramatic civic contributions to public health are not limited to a time in the U.S. when voluntary organizations flourished or to simple matters of campaign fundraising and volunteering. Into the perceived void of leadership by health authorities at the start of the HIV/AIDS epidemic stepped a number of community groups that both advocated and self-organized (when slow to emerge through formal institutions) health education and care delivery systems for patients suffering from the disease as well as it social stigma (5, 35). Community-based organizations fought for social policies that would prevent the spread of the epidemic and protect the rights of the infected. Grassroots organizers also played a key role in shaping government regulation of, and research into promising drug therapies, and they worked toward fair consumer pricing. Today, as a requirement of the 1990 Ryan White Care Act, people personally affected by HIV/AIDS sit alongside government leaders, health officials, and heads of community-based groups to help set local spending priorities for federal funds—whether primary medical care, case management services, or volunteer labor power (59).

The citizen role in reducing the scourge of HIV/AIDS is hardly limited to safe sex behaviors or to keeping one's children safe from chills or over-exertion in the case of polio, however critical these contributions may be the health of the individual and society. A genuine account of civic preparedness must span from the realm of individual protective behaviors, to the group actions of formal and informal volunteer networks, to the public deliberation of health emergency management policies and their implementation. Until now, the most "public" of public involvement efforts in health emergency management has occurred only on a small-scale experimental basis (36, 75). The U.S., thus, requires a concerted effort to institutionalize community engagement as the national standard for state and local health emergency planning.

National Initiative on Community Engagement for Public Health Preparedness

Current U.S. health emergency policies—at all levels of government—do not adequately reflect the civic infrastructure's proven contributions in disasters and epidemics. Nor have policymakers realized the even greater potential of consciously standing up, collaborating with, and regenerating trained networks of disaster-conscious constituents. The citizen role in emergencies may play an important rhetorical function in present political discussions, but this is not matched by a commensurate level of public funding. Two indices mentioned earlier are Citizens Corps' negligible operating budget in DHS, and the priority placed on mass risk communication capabilities in the HHS/CDC preparedness grants to state and local health agencies, rather than the more resource dependent approaches of community engagement.

Moreover, civic contributions in the management of health emergencies have been narrowly construed as private acts of stockpiling and ready households, not the more open, group actions of informing public health preparedness plans, gauging their outcomes, and making refinements. The structures for amassing the collective good of voluntarism are presently weak, and those for applying a community's judgment are non-existent. A conscious, deliberate, and well-funded effort will be necessary to reverse this trend. Some recent developments, however, represent opportunities for positive change.

The bipartisan-supported *Pandemic and All-Hazards Preparedness Act* (PAHPA) was signed into

law in December of 2006. This Act singled out "risk communication and public preparedness" as "essential public health security capabilities" (Sec. 103). It also made emergency preparedness awards to state and local health agencies via cooperative agreements with HHS/CDC contingent upon an explicit mechanism, such as an advisory committee, "to obtain public comment and input" on preparedness and response plans and their application (Sec. 201). If implemented well, PAHPA presents a ripe opportunity to advance local health emergency preparedness systems that collaborate with civic groups and incorporate citizen input, thus helping obtain what some have called a true "culture of preparedness."

Congress, when making appropriations for PAHPA, should fund public preparedness at a level commensurate with its status as "essential public health security capabilities." Specifically, Congress should authorize sufficient funds to support state/local health agencies in hiring the fulltime staff necessary for community engagement, to vitalize the Citizens Corps in more localities, and to support local community-based groups in devising emergency plans that pool resources and tap social networks. HHS and DHS—in their joint efforts to expand the Lessons Learned Information System as required by PAHPA—should facilitate the collection, analysis, and sharing of best practices related to civic engagement, volunteer mobilization, and other forms of public involvement in disaster and health emergency management.

Mayors, governors, and county executives can provide the political support and visibility necessary to institutionalize preparedness partnerships between civic groups and health and safety officials. Key actions include providing financial and programmatic support for a fulltime qualified coordinator within the health department (or emergency management office) with experience in community engagement, and assessing their own administration's means to engage local opinion leaders and citizens at-large (e.g., advisory boards, neighborhood liaison offices, health education and outreach staff) and how these might be tapped for health emergency objectives. Community engagement should be part of present pandemic flu preparedness efforts, with special attention to devising socially fair and acceptable plans to distribute scarce life-saving medical resources, care for sick people when hospitals become overburdened, and provide a safety net for people who have chronic illness and other special needs.

Heads of community-based groups need not wait to be invited to the health emergency planning table. They can contact their political representatives, as well as local health officers and emergency managers, to offer advice on a community engagement structure. At the same time, they can work with officials immediately to obtain advice on their own continuity planning, ascertain pre-event protocols for volunteer integration, and discuss how the group might mobilize its own network as part of a pre-event education campaign and/or crisis and recovery support system.

Conclusion

Deliberate planning for the smart flow of meaningful information among officials and with the public proves requisite for improving the nation's ability to handle both emergent and familiar health threats. The call for citizens' active engagement in the formulation and implementation of health policy for major emergencies represents only one of many open government challenges within the larger biodefense context. Greater transparency in preparedness goals and budgets, robust biosafety systems for laboratories, and clarification of the rationale for major biomedical investments can also help assure that protections against biological attacks and other extreme health events produce their intended results, without unacceptable costs to the public's health and other core U.S. values and objectives.

BIBLIOGRAPHY

1. News release, American Association for Retired Persons, AARP offers tips to help older Americans prepare for emergencies (September 6, 2006), *available at* http://www.aarp.org/research/press-center/presscurrentnews/preparing_for_emergencies.html (last accessed Oct. 17, 2006).

2. American Red Cross, *Be prepared – American Red Cross preparedness information*, *available at* http://www.redcross.org/services/disaster/0,1082,0_500_,00.html (last accessed Oct. 15, 2006).

3. G. J. Annas, *Bioterrorism, public health, and civil liberties,* New England J. of Medicine, 346(17):1337-1342 (2002).

4. M. J. Armstrong, *Back to the future: Charting the course for Project Impact,* Natural Hazards Rev., Aug. 2000 August, 138-144.

5. R. Bayer, *The dependent center: the first decade of the AIDS epidemic in New York City, in* Hives of Sickness: Public Health and Epidemics in New York City 131-150 (D. Rosner ed., Rutgers Univ. Press).

6. T. C. Beierle, *The benefits and costs of disclosing information about risks: what do we know about right-to-know?* Risk Analysis 24(2):335-346 (2004).

7. J. C. Belke & D. Y. Dietrich, *The post-Bhopal and post-9/11 transformations in chemical emergency prevention and response policy in the United States*, J. of Loss Prevention in the Process Industries 18(4-6):375-379 (2005).

8. Centers for Disease Control and Prevention, *Crisis and Emergency Risk Communication,* Atlanta, GA, 2002.

9. S. Chambers, *Deliberative democracy theory,* Annual Rev. Political Sci. 6:307-26 (2003).

10. K. Chekouras, *Balancing national security with a community's right-to-know: maintaining public access to environmental information through EPCRA's non-preemption clause,* B.C. Envtl. Aff. L. Rev. 34(1):107-142 (2007).

11. L. Clarke, *Panic: Myth or reality?* Contexts 21–6, Fall 2002.

12. Collaborating Agencies Responding to Disasters, *available at* http://www.firstvictims.org/whoweare.html (last accessed Oct. 17, 2006).

13. Committee on Disaster Research in the Social Sciences, *Facing Hazards and Disasters: Understanding Human Dimensions*, Washington, D.C., Nat'l Academies Press, 2006.

14. L. E. Davis, T. LaTourrette, & D. E. Mosher, *et al, Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks*, Santa Monica, CA, RAND Public Safety and Justice, 2003.

15. M. X. Delli Carpini, F. L Cook, & L. R. Jacobs, *Public deliberation, discursive participation, and citizen engagement*, Annual Rev. Political Sci. 7:315-44 (2004).

16. A. J. Dory, *Civil Security: Americans and the Challenge of Homeland Security*, Washington, D.C., Center for Strategic and International Studies, Sept. 2003.

17. R. R. Dynes, *Community emergency planning: false assumptions and inappropriate analogies,* Int'l J. of Mass Emergencies & Disasters 12(2):141-158 (1994).

18. N. Eliasoph, Avoiding Politics: How Americans Produce Apathy in Everyday Life (Cambridge Univ. Press 1999).

19. N. Ethiel ed. *Terrorism: Informing the Public*, McCormick Tribune Foundation, 2002.

20. C. Franco, & S. Deitch, *Billions for biodefense: federal agency biodefense funding, FY2007-FY2008,* Biosecurity & Bioterrorism 5(2):117-133 (2007).

21. A. Fung, M. Graham, & D. Weil, Full Disclosure: The Perils and Promise of Transparency. (Cambridge Univ. Press 2007).

22. T. R. Gablehouse, *The role of local communities in chemical accident prevention and preparedness,* J. of Loss Prevention in the Process Industries 18:549-552 (2005).

23. T. Glass, & M. Schoch-Spana, *Bioterrorism and the public: how to vaccinate a city against panic?* Clinical Infectious Diseases 34:217-223 (2002).

24. J. Goldman, *Balancing in a crisis? Bioterrorism, public health, and privacy*, *in* Lost Liberties: Ashcroft and the Assault on Personal Freedom 161-183 (C. Brown ed., New Press, 2003).

25. M. Graham, *The information wars: terrorism has become a pretext for a new culture of secrecy,* The Atlantic Monthly 36,38, Sept. 2002.

26. G. K. Gronvall, J. Fitzgerald, & A. Chamberlain, *et al, High-containment biodefense research laboratories: meeting report and center recommendations,* Biosecurity & Bioterrorism 5(1):75-85 (2007).

27. E. Gursky, Progress and Peril: Bioterrorism Preparedness Dollars and Public Health (The Century Foundation, 2003).

28. E. Hammond, Testimony to the Subcommittee on Oversight and Investigations of the House Energy and Commerce Committee for the hearing, *Germs, viruses, and secrets: the silent proliferation of bio-laboratories in the United States*, Oct. 4, 2007.

29. J. R. Harrald, *Emergency management restructured: intended and unintended outcomes of actions taken since 9/11, in* Emergency Management: The American Experience 1900-2005 161-183. (C. B. Rubin ed., Public Entity Risk Institute, 2007).

30. H. Harvey, *An Overview of the U.S. Public Health System in the Context of Bioterrorism*, Congressional Research Service, RL31719, updated Feb. 11, 2004.

31. K. Hebert, N. Henderson, & E. A. Gursky, *Building preparedness by improving fiscal accountability,* J. Pub. Health Management Practice 13(2):200-201 (2007).

32. D. A. Henderson, *The looming threat of bioterrorism,* Science 283:1279-1282.

33. J. R. Hibbing, E. Theiss-Morse, Stealth democracy: American's beliefs about how government should work (Cambridge Univ. Press, 2002).

34. J. G. Hodge, E. F. Brown, & J. P. O'Connell, *The HIPAA privacy rule and bioterrorism planning, prevention, and response,* Biosecurity & Bioterrorism 2(2):73-80 (2004).

35. The Social Impact of AIDS in the United States (A. R. Jonsen, J. Stryker eds., National Academy Press, 1993).

36. R. D. Lasker, N. D. Hunter, S. E. Francis, With the Public's Knowledge, We Can Make Sheltering in Place Possible (New York Academy of Medicine, 2007).

37. P. C. Light, *The Katrina effect on American preparedness,* New York University Center from Catastrophe Preparedness and Response, Nov. 2006 *available at* http://www.nyu.edu/ccpr/katrina-effect.pdf (last accessed Dec. 11, 2006).

38. M. K. Lindell, *Are local emergency planning committees effective in developing community disaster preparedness?* Int'l J. of Mass Emergencies & Disasters 12(2):159-182 (1994).

39. N. Lurie, J. Wasserman, & C. D Nelson, *Public health preparedness: evolution or revolution?* Health Affairs 25(4):935-945 (2006).

40. R. O'Leary, *The Emergency Planning and Community Right-to-Know Act: Ten public management challenges for state and local governments*, Pub. Productivity & Management Rev. 18(3):293-310 (1995).

41. D. M. Oshinsky, Polio: An American Story (Oxford Univ. Press, 2005).

42. L. Pearce, *The value of public participation during a hazard, impact, risk and vulnerability (HIRV) analysis,* Mitigation and Adaptation Strategies for Global Chance 10:411-441 (2005).

43. L. Pearce, *Disaster management and community planning, and public participation: how to achieve sustainable hazard mitigation,* Nat. Hazards 28:211-228 (2003).

44. A. M. Pearson, Testimony to the Subcommittee on Oversight and Investigations of the House Energy and Commerce Committee for the hearing, *Germs, viruses, and secrets: the silent proliferation of bio-laboratories in the United States,* Oct. 4, 2007.

45. A. J. Perrin, Citizen Speak: The Democratic Imagination in American Life (Chicago Univ. Press, 2006).

46. C. S. Prater & M. K. Lindell, *Politics of hazard mitigation,* Nat. Hazards Rev. May 2000, 73-82.

47. R. Putnam, Bowling Alone: The Collapse and Revival of American Community (Simon & Schuster, 2000).

48. E. L. Quarantelli, *The sociology of panic, in* Int'l Encyclopedia of the Social and Behavioral Sci. 11020–30 (N. Smelser & P. B. Baltes eds., Pergamon Press, 2001).

49. S. C. Quinn, T. Thomas, & C. McAllister, *Postal workers' perspectives on communication during the anthrax attack,* Biosecurity & Bioterrorism 3(3):207-215 (2005).

50. K. Rhodes, Testimony before the Subcommittee on Oversight and Investigations of the House Energy and Commerce Committee at the hearing, *Germs, viruses, and secrets: the silent proliferation of bio-laboratories in the United States,* GAO-08-108T, Oct. 4, 2007.

51. R. C. Rich, M. Edelstein, W. K. Hallman *et al, Citizen participation and empowerment: the case of local environmental hazards,* Am. J. of Community Psychology 23(5):657-676 (1995).

52. D. Rosner & G. Markowitz, Are We Ready?: Public Health Since 9/11 (Univ. of California Press, 2006).

53. G. Rowe & L. J. Frewer, *A typology of public engagement mechanisms,* Sci., Technology, & Human Values 30(2):251-90 (2005).

54. L. J. Schierow, *Chemical Facility Security,* Congressional Research Service, RL31530, updated Aug. 2, 2006.

55. M. Schoch-Spana, *Public archetypes in U.S. counter-bioterrorist policy*, *in* Understanding and Responding to Terrorism 364-374 (H. Durmaz *et al* eds., NATO Security through Science Series, E:Human and Societal Dynamics – Volume 19, IOS Press, 2007).

56. M. Schoch-Spana, *Bioterrorism: U.S. public health and a secular apocalypse,* Anthropology Today 20(5):1-6 (2000).

57. M. Schoch-Spana, *Educating, informing and mobilizing the public*, *in* Terrorism and Public Health 118-135 (B. Levy & V. Sidel eds., Oxford Univ. Press, 2003).

58. M. Schoch-Spana, A. Chamberlain, & C. Franco, *et al*, *Disease, disaster, and democracy: the public's stake in health emergency planning*, Biosecurity & Bioterrorism 4(3):313-319 (2006).

59. M. Schoch-Spana, C. Franco, & J. B. Nuzzo, *et al*, on behalf of the Working Group on Community Engagement in Health Emergency Planning, *Community engagement: leadership tool for catastrophic health events*, Biosecurity & Bioterrorism 5(1):8-25 (2007).

60. T. Skocpol, Diminished democracy: From membership to management in American civic life (Univ. of Oklahoma Press, 2003).

61. V. W. Sidel, R. M. Gould, & H. W. Cohen, *Bioterrorism preparedness: cooptation of public health?* Medicine & Global Survival 7(2):80-87 (2001).

62. A. Smithson & L. A. Levy, Ataxia: The Chemical and Biological Terrorism Threat and the US Response (The Henry L. Stimson Center).

63. J. Sorenson, *Risk communication and terrorism,* Biosecurity & Bioterrorism 2(3):229-231 (2004).

64. B. Stein, T. L. Tanielian, & G. W. Ryan, *et al, A bitter pill to swallow: nonadherence with prophylactic antibiotics during the anthrax attacks and the role of private physicians,* Biosecurity & Bioterrorism 2(3):175-185 (2004).

65. E. Theiss-Morse & J. R. Hibbing, *Citizenship and civic engagement,* Annual Rev. Political Sci. 8:227-49 (2005).

66. K. Tierney, *Testimony regarding needed emergency management reforms*, J. of Homeland Security & Emergency Management 4(3): Article 15 (2007).

67. Trust for America's Health, Ready or Not?: Protecting the Public's Health from Disease, Disasters, and Bioterrorism (TFAH, 2006).

68. U.S. Dep't of Homeland Security, http://www.ready.gov.

69. U.S. Dep't of Health and Human Services, *Communicating in a Crisis: Risk Communication Guidelines for Public Officials,* 2002.

70. U.S. Gov't Accountability Office, *Bioterrorism: Information on Jurisdictions' Expenditure and Reported Obligation of Program Funds,* GAO-05-239, 2005.

71. T. Wachtendorf, *Building community partnerships toward a national mitigation effort: Inter-organizational collaboration in the Proj-*

ect Impact initiative, DRC preliminary paper #306, Disaster Research Center, Univ. of Delaware, 2000.

72. R. Ward & G. Wamsley, *From a painful past to an uncertain future, in* Emergency Management: The American Experience 1900-2005, 207-241 (C. B. Rubin ed., Public Entity Risk Institute, 2007).

73. W. L. Waugh & R. T. Sylves, *Organizing the war on terrorism,* Pub. Admin. Rev. 62, special issue: 146-153 (2002).

74. Working Group on 'Governance Dilemmas' in Bioterrorism Response, *Leading during bioattacks and epidemics with the public's trust and help*, Biosecurity and Bioterrorism 2(1):25-40 (2004).

75. Public Engagement Pilot Project on Pandemic Influenza, *Citizen voices on pandemic flu choices: A report of the public engagement pilot project on pandemic influenza,* Dec. 2005, *available at* http://ppc.unl.edu/publications/documents/PEPPPI_FINALREPORT_DEC_2005.pdf.

3.3 The Texas Public Information Act and Bioresearch: Application and Implications

by Joseph R. Larsen

Legislation is always an exercise in the art of the possible. There are usually many competing interests, often irreconcilable interests, to balance and a paucity of empirical evidence about how much information *should be* released. In addition, even if legislators had objective information regarding application of the underlying principles at issue, the actual result of the legislation is often quite wide of the mark. With any legislative framework, the law of unintended consequences looms large, and the actual result depends in large part upon the procedural and litigation realities which underlie the application of the law. Finally, the integrity of any system depends in large part on the integrity of its components. In the context of open government laws, this integrity depends at least in part on honesty in fact of the governmental bodies involved.

The interface between the Texas Public Information Act, with its emphasis on the right of the citizens to know what their governmental institutions are doing, and doing with their money, and public institutions involved in bioresearch, with their own competing interests of security, intellectual property, and intellectual freedom, is a fruitful microcosm to review as it sheds light on many of the larger issues often unexamined regarding how an open society is to provide for its own security. This paper will provide a brief study of the actual application of several statutes meant to govern release of information in the possession of public institutions funded in large part by public money, and also to discuss the particular instance of one Texas institution, Texas A&M, to properly report a reportable occurrence and, in response to a request to information, to acknowledge the existence of responsive information.

The Texas Public Information Act

This statutory framework, modeled generally after the federal Freedom of Information Act, was passed in 1973 as the Open Records Act in the wake of the "Sharpstown" banking scandal which implicated several sitting legislators. It was renamed the Public Information Act ("PIA") in 1995 when it was rewritten to require release of information in the hands of private entities kept on behalf of governmental bodies and to better define access to electronic information. *See generally,* Tex. Gov't Code § 552.001 *et seq*.

The PIA mandates that all information kept by or on behalf of governmental bodies is public unless it falls within an exception to the PIA. However, there are a number of statutory exceptions to the PIA, and the number grows with each legisla-

Figure 1
Civic Infrastructure Capacities to Remedy Disasters and Epidemics[59]

Multi-frequency communications network to reach dispersed and diverse populations

- "Live" since June '05, Flu Wiki (www.fluwikie.com) is a virtual non-profit that helps local communities prepare for and perhaps cope with a possible flu pandemic by tapping the skills, knowledge, and desire to learn of its diverse users and core moderator group.
- Salon Voices, an innovative non-profit in Washington (DC), engages the hair salon culture of the African-American community and equips cosmetologists with information and internet connections to educate customers on HIV/AIDS, reproductive health, and parenting.

Social circuitry to energize trust between authorities and communities at-large

- CARD - Collaborating Agencies Responding to Disasters (Alameda County, CA) emerged after the Loma Prieta earthquake to train and unite service providers as a safety net for people with limited ability to address their own disaster-related needs—seniors, children, the disabled, the homeless, non-English speakers, and low income families. CARD has subsequently developed an alternative curriculum, devoid of fear-based messages, emphasizing community building, leadership cultivation, and economic development strategies.
- St. Philip of Jesus Parish and the University of the Incarnate Word in San Antonio (TX) team up nursing faculty and students with *promotoras de salud* (lay community health workers) to reach a near-by, wary and under-served Hispanic population through health programs held at the church hall, neighborhood barbeques, and subsidized housing for the elderly.

Collective wisdom to set policy priorities and inform values-laden health policy decisions

- In 2006, the Public Engagement Project on Community Control Measures for Pandemic Influenza held public deliberations – involving national stakeholder and regionally diverse citizens at-large – about which non-pharmaceutical measures should be implemented early on to slow flu's spread, and about ways to mitigate the adverse economic and social effects of these interventions.
- As a requirement of the 1990 Ryan White Care Act, people personally affected by HIV/AIDS sit alongside government leaders, public health officials, and heads of community-based organizations to help set local spending priorities for federal funds—whether primary medical care, case management services, volunteer labor power, etc.

Local knowledge to improve feasibility, reliability, and acceptability of disaster plans

- Residents of Grand Bayou (LA), a Cajun and Native American ocean-farming community, have partnered with state and local government, business, the faith community, and university-based experts to tackle mounting coastal dangers; one such effort is hazard mapping that incorporates indigenous knowledge about historic environmental transformations.
- During the 1947 smallpox outbreak, NYC health officials vaccinated >6.3mil people in 4 weeks (>5mil alone in the first 2 weeks) using private physicians and volunteers from the Red Cross, teachers' groups, women's clubs, and civil defense groups; this partnership helped staff free clinics in 12 hospitals, 84 police precincts, and every public and parochial school.

Operational support for professional responders during crisis and recovery periods

- The Harris County (TX) Citizens Corps helped manage 60,000 volunteers in setting up a "mini-city" at the Houston Astrodome to host 65,000 Katrina evacuees in 2005.
- In the 1960s, the Junior Chamber of Commerce in cooperation with health departments launched "Sabin on Sunday," a mass vaccination program that reached 80–90% of the target population—a critical step in eliminating polio in the U.S.

Self-organized, innovative solutions when unforeseen needs arise

- After the emergency services leadership evacuated the area, a Plaquemines employee took charge by phoning around the south parish to locate people stranded by the Hurricane Katrina storm surge and to commandeer boats, keys, and gasoline for a search-and-rescue "Cajun Navy."
- Responding to calls from the American Council of Education and the Association of American Universities, more than 1,000 U.S. colleges took in >18,500 students displaced from the 6 Louisiana colleges closed by Hurricane Katrina—with offers of reduced or free tuition.

Rooted-ness in place that personalizes communitywide recovery and amasses resilience

- Some Katrina-weary New Orleans residents were tentative about rebuilding due to demolition, debris removal, and reconstruction challenges; neighbors' exchanges of labor, expertise, tools and equipment, shelter, and childcare have made rebuilding a physical possibility and conveyed social commitments to the future of their communities.
- Greater Seattle (WA) residents, businesses, and emergency managers collaborated on "Disaster Saturday," a preparedness and survival training on earthquakes for the public. By the time the 6.8 Nisqually earthquake hit in 2001, 1,000 people had taken the training, and at least 300 of them had retrofitted their homes, none of which were damaged in the quake.

Tax revenue base and in-kind contributions that help mitigate extreme event losses

- In a multi-day blitz, 29,000 Berkeley households received disaster readiness door hangers in 2006; Disaster Resistant Berkeley (a former Project Impact recipient) funded the campaign from a special preparedness city tax and used student volunteers from the University of California.
- "McReady OK!"—a private-public collaboration in the heart of Tornado Alley—has made free spring storm survival information available in every McDonald's restaurant in Oklahoma, reaching upwards of 150,000 customers a day for an entire month each year since 2003.

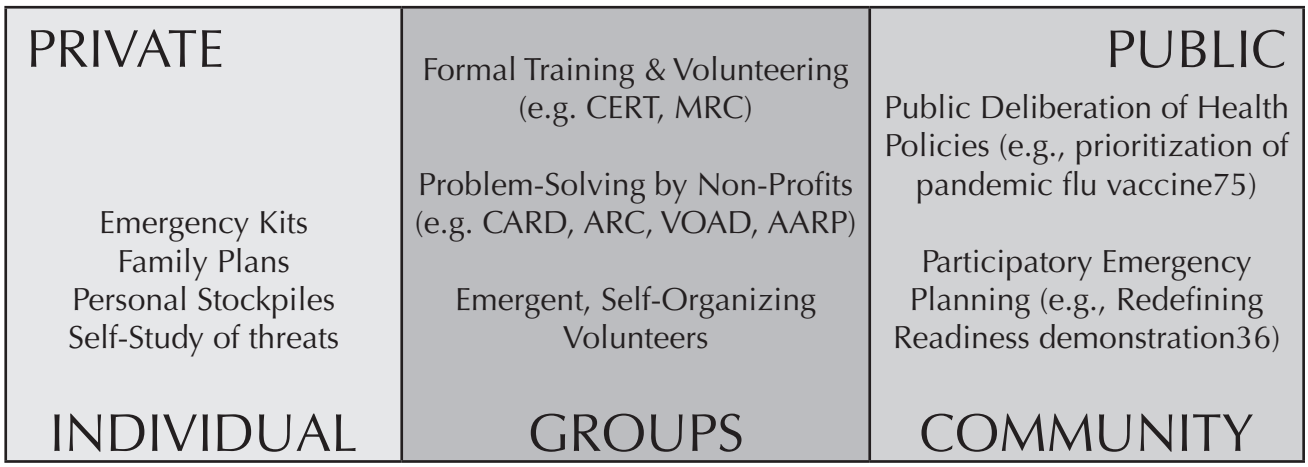

Figure 2. *Civil Preparedness Continuum*

tive session. The first of these exceptions requires a governmental body to withhold all information considered "confidential by law." This exception brings in a plethora of confidentiality statutes, including the two statutes examined by this paper, as well common law constructs such as trade secrets and right to privacy.

The Texas PIA is unique among state freedom of information laws in that the state attorney general ("A.G.") serves as essentially an ombudsman regarding each request. A governmental body, if it seeks to withhold information, is required to seek an attorney general ruling within ten working days. The attorney general issues a ruling within 45 working days of the governmental body's request. As a result, Texas has A.G. rulings on specific legislation that shed some light on the actual application of some statutes that may not, for reasons of time and/or resources, have resulted in a reported court decision. A governmental body that feels the attorney general has ruled in error may contest the ruling by filing a lawsuit against the Attorney General. The actual procedural and evidentiary issues involved in taking such a case to trial will also be reviewed.

A Typical Request

This first part of this paper will focus on some of the information sought by a typical request, two of the statutes raised by the governmental body to withhold the requested information, and Texas Attorney General Letter Ruling, OR2007-00489, which opined on the assertions made by the governmental body. Finally, I will look at how these same issues would be dealt with at the next level—litigation. This examination will be useful as a check on our expectations as to what sort of confidentiality is possible and advisable given the various and conflicting goals of the governmental bodies and the realities of our legal system. It is hoped that his study will be a fresh perspective on the implications of the legislative schemes we have enacted for reasons often at cross-purposes with each other, and for future proposed legislation.

The attorney general summarized the information sought by the requester, a well-known watchdog group, as follows:

> [T]en categories of information concerning the UTMB Institutional Biosafety Committee; notifications of use involving biosafety considerations; records of occupational exposures and/or laboratory-acquired infections; Dr. Stanley Lemon's participation on the National Science Advisory Board for Biosecurity; meetings of the New England biodefense regional center of excellence; correspondence with the Southwest Foundation for Biomedical Research and with Dr. Rick Lyons; research contracts with other institutions; and other matters.

Much of the information responsive to this request consists of approved and unapproved applications for grants for specific bioresearch proposals. With regard to this specific information, the exceptions raised by the governmental body fall into two categories: (1) intellectual property; and (2) security.

1. Intellectual Property

The increasing privatization of the public sphere can be seen not only in the increasing use of private vendors to perform governmental services, from maintaining government databases to providing military support, but also by the morphing of governmental bodies themselves into for profit actors. The latter is due in part, to the simple fact that the amount of dedicated public funds is simply insufficient to maintain public research institutions. Public bodies are increasingly seen as competing in the private sector for available resources, and competing with the private sector to profit from intellectual property. Indeed, research institutions are increasingly being asked to live off what they kill, so to speak, and are encouraged to

obtain patent protection for research results with potential commercial application.

In connection with this, in 1985 the Texas legislature passed the statute now codified at Tex. Educ. Code § 51.914:

> In order to protect the actual or potential value, the following information shall be confidential and shall not be subject to disclosure under [the Act], or otherwise:
>
> (1) all information relating to a product, device, or process, the application or use of such a product, device, or process, and all technological and scientific information (including computer programs) developed in whole or in part at a state institution of higher education, regardless of whether patentable or capable of being registered under copyright or trademark laws, that have a potential for being sold, traded, or licensed for a fee; [or]
>
> (2) any information relating to a product, device, or process, the application or use of such product, device, or process, and any technological and scientific information (including computer programs) that is the proprietary information of a person, partnership, corporation, or federal agency that has been disclosed to an institution of higher education solely for the purposes of a written research contract or grant that contains a provision prohibiting the institution of higher education from disclosing such proprietary information to third persons or parties[.]

In connection with the government body's request to withhold information under this exception, the A.G. generally concurred, holding:

> This office has stated that in considering whether requested information has "a potential for being sold, traded, or licensed for a fee," we will rely on a university's assertion that the information has this potential. Section 51.94 is applicable only to information "developed in whole or in part at a state institution of higher education." Tex. Educ. Code § 51.914(1).

This letter ruling reflects the fact that the attorney general is not empowered to make findings of fact. Of course, at the level of review by the attorney general, this clearly puts the governmental body in the driver's seat with regard to claims of intellectual property. This singular limitation renders almost ineffective the mandate that the PIA is to be liberally interpreted to favor release of information, and its corollary that confidentiality statutes are to be narrowly construed.

However, moving this issue into a court of law brings its own set of difficulties. Whether or not particular "information" has the "potential" for being "sold, traded, or licensed for a fee" will almost certainly have to be proven by expert testimony. Expert testimony is subject to exacting standards in order to be deemed helpful to the trier of fact. *See E.I. du Pont Nemours & Co. v. Robinson*, 923 S.W.2d 549, 556-57 (Tex. 1995). Further, an expert must usually express that a certain matter is "reasonably" probable, that is, more probable than not. Finally, the expert will have to articulate the factual basis underlying his or her conclusion. *See, e.g., Lyondell Petrochem Co. v. Fluor Daniel, Inc.,* 888 S.W.2d 547, 554 (Tex. App.—Houston [1st Dist.] 1994, writ denied.).

It is hard to square the language of this statute, expressed in "potentialities," and the burden of proof that requires a governmental body to show it is more probable than not that particular information falls within an asserted exception. As a matter of statutory construction, how is a court to "narrowly read" a confidentiality statute that requires proof of "potential" for being sold or licensed?" To take a more concrete example, evidence of how

much money a start up business was expected to make is often rejected by a court as speculative unless there is some solid historical information from which one can make a projection.

Intellectual property often comes up in the context of a public information act request. However, these claims are usually defended by third parties who have provided information to a governmental body as part of a bid or package for approval to do business. Procedurally, the governmental body advises the third party of the request, and it is the third party's obligation to establish the claims before the attorney general, or prove them in court. If the claim is that the information is a trade secret, the third party must make its case on the traditional common law factors: (1) the extent to which the information is known by employees and others involved in the company's business; (2) the extent to which it is know by employees and others involved in the business; (3) the extent of measures taken to guard the secrecy of the information; (4) the value of the information to the company and its competitors; (5) the amount of money or effort expended in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others. *See* Tex. Gov't Code § 110(a); *Hyde v. Huffines*, 314 S.W.2d 763, 776 (Tex. 1958). Alternatively, a third party may demonstrate "based on specific factual evidence that disclosure would cause substantial competitive harm to the person from whom it was obtained." Tex. Gov't Code § 110(b); Tex. Att'y Gen. Op. ORD No. 659 at 2 (1990).

That an institution of higher education is granted far more sweeping protection for its intellectual property than third parties who share information with the government is not only inconsistent, but there is obviously a tension in the very idea of a publicly owned institution having intellectual property rights, and free access to publicly financed research is not only consistent with the public policy rationale for such research, but the obverse, roping off the public and/or competing institutions from this information runs against the increasingly outmoded concept of open scientific debate. Further, the current paradigm has the unintended consequence of choking off the flow of information *to* these institutions from countries and organizations that fear that information freely given will become the property of the institution, foreclosing or limiting the power to use it freely or at all in the future.

In this regard, as pointed out in an Op-Ed piece by Michael Crichton published on February 13 of this year in the New York Times entitled "Patenting Life," when SARS was spreading across the globe, "medical researchers hesitated to study it—because of patent concerns. There is no clearer indication that gene patents block innovation, inhibit research and put us all at risk." The same is surely true when researcher or doctor will refuse to provide information to a research institute because of concerns the information freely granted will later become available only upon execution of a license.

2. Security

Perhaps it is not surprising that much of the very information that this and similarly situated governmental bodies seek to withhold on the basis of its potential commercial value is also claimed as information that should be withheld from release because it could be useful to terrorists. While filing an application for patent protection for information is at odds with making sure it doesn't "fall into the hands of the bad guys," research institutions will nevertheless claim both exceptions for the same information. With regard to bioresearch (and other "dual purpose research"), the specific statutes involved and the attorney general's holding on the issues presented are as follows:

> Section 418.178, as added to chapter 418 of the Government Code as part of the Texas Homeland Security Act, provides as follows:

> (a) In this section, "explosive weapon" has the meaning assigned by Section 46.01, Penal Code.
>
> (b) Information is confidential if it is information collected, assembled, or maintained by or for a governmental entity and:
>
> > (1) Is more than likely to assist in the construction or assembly of an explosive weapon or a chemical, biological, radiological, or nuclear weapon of mass destruction; or
> >
> > (2) Indicates the specific location of:
> >
> > > (A) A chemical, biological agent, toxin, or radioactive material that is more than likely to be used in the construction or assembly of such a weapon; or
> > >
> > > (B) Unpublished information relating to a potential vaccine or to a device that detects biological agents or toxins.

Tex. Gov't Code § 418.178. The fact that information may generally relate to biological toxins does not make the information *per se* confidential under section 418.178. *See* Open Records Decision No. 649 at 3 (1996) (language of confidentiality provision controls scope of its protection). As with any confidentiality statute, a governmental body asserting section 418.178 must adequately explain how the responsive records fall within the scope of that provision. *See* Tex. Gov't Code § 552.301(e)(1)(A) (governmental body must explain how claimed exception to disclosure applies).

UTMB asserts that section 418.178 is applicable to information encompassed by items 4, 8, and 9 of the request. You contend that some of the information in question reveals the location of biological agents or toxins that have potential for use in terrorist plots and thus is protected by section 418.178(b)(2)(B). You also argue that section 418.178(b)(2)(B) encompasses responsive information that relates to antidote research for exposure to certain bio-toxins. SFBR contends that the names of biological agents and/or toxins and of employees conducting research concerning potential vaccines are protected by section 418.178(b)(2). We note that section 418.178 is applicable only to (1) information that is more than likely to assist in the construction or assembly of an explosive weapon or weapon of mass destruction and (2) information indicating the specific location of certain materials that are potentially useful in constructing or assembling such a weapon or of unpublished information relating to a potential vaccine or a device that detects biological agents or toxins. We have marked information revealing the location of toxins that is confidential under section 418.178 of the Government Code and must therefore be withheld under section 552.101. As neither UTMB nor SFBR has explained how or why section 418.178 encompasses any of the remaining information at issue, UTMB may not withhold any other information on that basis.

Again, at the level of review of the Texas Attorney General, facts asserted by the governmental body are accepted as true. Despite this, and perhaps because this statute is written more consistent with the governmental body's burden of proof that information be "*more than likely* to assist in the construction or assembly of a . . . biological . . . weapon of mass destruction," the attorney general found the governmental body had "not explained" how much of the claimed information fell with the asserted exception.

Because in this, and many instances, the governmental body challenged the AG's ruling in court, it is useful to review how this issue might be dealt with before a court of law. Again, whether information could "more than likely" assist in construction of WMD is an opinion which will have to be given by an expert (possibly the same expert could testify that the information has commercial application), subject to the same limitations and constraints discussed above.

The scale of such a trial is large indeed, as this request and similar ones from other watchdog groups and media typically involve many applications and reports and thousands of pages. Because the matters at issue are claimed to be secret, discovery must be done pursuant to a protective order and some pleadings filed under seal and reviewed *in camera,* that is, by the court in chambers.

The daunting prospect of a many-week trial for release of public information that looks a lot like a trial for misappropriation of trade secrets gives pause as to the efficacy of these laws. But even aside from that, there are several assumptions underlying laws, like this, whose purpose is to keep information from "failing into the hands of the bad guys." The first is that you can actually prevent the bad guys from gaining access to the information by limiting public access to the information; the second is that the information would be more useful to the bad guys to attack us than it would be to the public to insure our defense.

There is a dearth of research on the issue, but a law review article by Peter Swire at least gives a framework with which to get past the rhetoric that is normally offered as analysis. *See* Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 Houston L. Rev. 133 (2006). Swire points out similarities between *revealing* software code to *prevent* breaches of security, as is done with LINUX software, and releasing information related to military or national security, again to *prevent* breaches of security. While there is clearly information to which the public should *not* have access, for example tactical plans that would use the element of surprise, as often as not this information is broadcast by the government itself, such as our battle plans in the Iraq theatre of war, for purposes of political persuasion. The recent stunning premature disclosure, by the Bush Administration, of an Osama Bin Laden video that had been provided to them by SITE Intelligence Group is another instance of the disconnect between the rhetoric regarding withholding information for national security and the reality of getting information out to influence public opinion. On the other hand, information that could help address security problems through greater public awareness and public pressure is often withheld.

There is No Responsive Information

The natural human tendency is to attempt to cover over mistakes and to consolidate power through operating without oversight. Where funding is involved, the temptation to conceal, falsify, or simply fail to keep records can be overwhelming.

Some readers of this paper may ask why a requester needs to see all this information in the first place. I have already discussed some of the public policy arguments, both for security and governance, as to why open access is always preferable. Aside from this, requesters have good reason to be suspicious of claims of governmental bodies that information responsive to a request does not exist. Often, the only way the watchdog learns of the existence of information is through reference to it in another document. Thus, requesters often cast a wide net.

The widely reported, though not by the governmental body, incident involving exposure to and infection by the brucella bacteria at Texas A&M is a case in point, but it is hardly unique. *See, e.g., More than 100 incidents reported at*

labs handling deadly germs, Austin American-Statesman, Oct. 2, 2007.

While the specifics of the exposure, diagnosis, request for information, initial denial of that there was any responsive information, eventual release, and subsequent events, including the CDC cease and desist letter and site visits, may be accessed at the website of The Sunshine Project, it is worth recounting in summary form here.

The Sunshine Project filed its Texas Public Information Act request on October 24, 2006 with Texas A&M for (among other items) "*All records on possible or actual occupational exposures and/or laboratory-acquired infections with risk group 2 (RG2) or higher agents at TAMU, from 1 January 2000 through the present*."

Texas A&M requested a ruling from the attorney general along the lines of the procedure outlined above, asserting (principally) Tex. Gov't Code § 418.178 as an exception. This resulted in Attorney General Letter Ruling OR2007-01189 in which the attorney general again observed that the fact that "information may generally relate to biological toxins does not make the information *per se* confidential" and that only *specific* locations may be withheld under this statute. The attorney general ruled that the remaining information must be released.

Texas A&M had not timely requested the ruling, and OR2007-01189 was not issued until January 31, 2007. Further, when Texas A&M finally released responsive documents, it produced only one page that it claimed was the entirety of its records on all exposures over a period of nearly 7 years. Texas A&M took the position that it had released all the documents that had been located and were responsive to the request. However, the single document that was released identified an occupational exposure to brucella, with the necessary implication that additional documents were required by law to have been generated, in particular, an APHIS/CDC Form 3. And, of course, the existence of only a single piece of paper as a result of such an exposure was simply not credible. Only as a result of continual pressure and escalation by the requester did Texas A&M finally release additional information in its possession, and finally inform CDC of the incident.

An incident at Texas A&M involving exposure to Q Fever, and a dearth of information regarding the incident has come to light since the brucella incident. Yet, Texas A&M has produced no accident reports, lab paperwork, lessons learned, or modified operating procedures, for either the Q Fever or the Brucella accident.

These institutional shortfalls have consequences potentially as deadly as those which could result if a terrorist group were to obtain truly sensitive information regarding the programs at issue, or somehow breach the physical security of the institution. Further, it appears that watchdog groups and public interest are more reliable in enforcing compliance and safe practices that governmental oversight. To underscore this, three years ago, President Bush ordered the Homeland Security Department to consolidate biological threats uncovered by agencies such as Centers for Disease Control and Prevention into a central early warning system (the "National Bio-Surveillance Integration System"). However, the Inspector General found that the system has failed to provide "consistent leadership and staff support to ensure successful execution" of the program. *See*, *U.S. biological detection program falling short, report says*, Austin American-Statesman, Aug. 11, 2007.

Conclusion

The principal purpose of this paper is to show the difficulty in drafting legislation with the purpose of preventing release of information in the stated interest of security, and the even greater difficulty in applying the legislation to the facts of a given case, particularly where the information is volumi-

nous. On the other hand, information that should clearly be maintained and released, and which we should hope is not overly voluminous, that involving accidental exposures or other such incidents, is being withheld using broad statutes never meant to reach this information, or is simply claimed not to exist. In part, institutions are relying upon the general talisman of terrorist threats and homeland security to justify not releasing information regarding dual use technology to the public at large, and watchdog requesters in particular, even while the vigorously pursue commercial applications for the information at issue.

This suggests that the proper legislative approach should be, instead of a focus on what a governmental body may withhold, to set a baseline for what is expressly public and can never be withheld under any exception to the Public Information Act.

This baseline should include mandatory reporting of all significant accidents and near-accidents with the details of each incident, including the name of the lab and the agent involved. It should also include the following:

1) Common and scientific name(s) and descriptions (including structures and sequences) of species and strains.

2) Name(s) and descriptions (including origin, structures and sequences) of nucleic acids.

3) Name(s) and descriptions (including origin, structures and sequences) of genetic vectors.

4) Name(s) and descriptions of research reagents.

5) Name(s) of Principal Investigator(s) and collaborator(s).

6) Individual name(s), institution name(s), city, and country of any individual or entity that provides biological materials to governmental body.

7) Individual name(s), institution name(s), city, and country of any individual or entity to which governmental body provides any biological materials.

8) Biosafety level and risk group information.

9) Make, model, size, type, or other descriptions of lab equipment.

10) The name(s) of any human or veterinary (candidate) therapeutics or vaccines.

11) The species and breed of any laboratory animal.

12) Information on the production method(s) and quantity(ies) of biological agents held or produced by governmental body.

With regard to grant applications:

1) Any portion of the grant abstract and other summary information.

2) Financial data.

3) The proposed grant term (length of time, start and end dates, etc).

4) Bibliographical information.

5) Descriptions of the problem being addressed.

6) Descriptions of past research.

7) Descriptions of research not conducted at governmental body.

8) Descriptions of the goals of research.

9) Biographical sketches (resumes) except for home addresses, home phone numbers, and social security numbers.

Not only would setting a baseline along these lines make unnecessary much of the intensive and wasteful struggle between watchdog groups and governmental bodies with regard to release of information, but it would make clear to the institutions involved that lack of transparency is not an option.

Chapter 4

Cyber Security

Synopsis

4.1 Beyond Practical Obscurity: Building Sound Privacy, Security and Open Government Policy in the Age of the Internet

by Ari Schwartz[1]

Abstract

The concept of "practical obscurity"—in which sensitive documents are theoretically attainable, but in practice remain of reach to ordinary citizens—served a purpose for over a decade, but has become increasingly unworkable as a matter of policy in the Internet age. Like the boy with his finger in the dyke, governments that attempt to keep publicly accessible data from reaching the Internet are fighting a losing battle. When possible, governments should take detailed inventories—not only of the information that they currently make available—but also of all the information that they collect from citizens. From those inventories they should make reasonable determinations about the potential harms of associated with releasing certain types of information. When a potential for harm is identified, the first choice should be to review the purpose of collecting that piece of information and stop collecting it if possible. If the collection of that potentially harmful information is deemed important for a legitimate government function, then governments should establish adequate safeguards for the sensitive data. Where no practical solution exists, governments will have to explore placing use limitations on the distribution of certain documents despite the fact that such limitations are difficult to legislate and enforce without incurring unintended consequences.

I. Introduction

In the pivotal 1989 case *Department of Justice v. Reporters Committee for the Freedom of the Press*, the U.S. Supreme Court introduced the idea of "practical obscurity" into the policy lexicon.[2]

The case centered on a reporter who had submitted a Freedom of Information Act (FOIA) request for information on the owners of a company that had received politically suspect defense contracts from the FBI. The Bureau complied with much of the request but would not provide one of the owner's rap sheets because it would have violated the privacy exemption to FOIA. A lower court upheld the FBI's decision. The U.S. Court of Appeals then overturned the decision suggesting that a FOIA requester could compile these same records from individual government agencies.[3]

1 Ari Schwartz is Deputy Director at the Center for Democracy and Technology in Washington, DC. http://www.cdt.org.

2 *See Department of Justice v. Reporters Committee of Freedom of the Press*, 489 U.S. 749 (1989).

3 *Reporters Committee for the Freedom of the Press v. US Dept. of Justice*, 816 F.2d 730, 740 (1987).

In a clearly worded decision, Justice John Paul Stevens wrote for a unanimous court that ruled in favor of the government's position that "practical obscurity" limits access to documents spread around the country in a way not possible with a single rap sheet:

> [P]lainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.[4]

Providing direct access to the same information in a different format changes the impact of making records public. Therefore, governments may establish different policies that make information accessible, but not too accessible, after they weigh the potential downsides of broader access. On the other hand, it is important to note that the court did not suggest that all documents containing privacy-sensitive information should be held in practical obscurity, but rather maintained that "[t]he privacy interest in maintaining the practical obscurity of rap-sheet information will always be high."[5]

In summary, the "practical obscurity" of government document protects the privacy of individuals to the extent that it requires major, inconvenient effort on the part of an information seeker to gather very private details about an individual held by the government.

Observers have noted that the concept of practical obscurity has been an important policy concept used regularly not only in FOIA privacy exemption decisions, but also in other policy determinations.[6] In fact, the precedent set by the Reporters Committee case has had an influence even beyond its impact on privacy, such as providing access to the risks from chemical plant or sensitive geographic information system (GIS) data. For example, in 1999 Congress passed a law that stopped the U.S. Environmental Protection Agency (EPA) from publishing certain data on the EPA web site or providing them in electronic form to FOIA requesters. This data in question - risk management plans (RMPs) for chemical companies collected under the Clean Air Act that included the so-called "worst case scenario" information about chemical plant disasters -- was limited out of fear that posting it online would allow terrorists easy access to the data.[7] Instead, Congress created a forced, practical obscurity of the RMPs by allowing public access only to a limited number of the actual reports through the federal depository library systems computers.[8]

While government policies rendering sensitive data practically obscure have increased, the futility of such policies has also become increasingly clear.[9] The cost of taking disparate sources of information (electronic or paper) and converting them into an electronic format that can be made available over the Internet has plummeted in recent years. Companies and organizations are now gathering information that was previously practi-

4 489 U.S. at 764.

5 489 U.S. at 762.

6 *See* Charles N. Davis, PhD, *Electronic Access to Information and the Privacy Paradox: Rethinking 'Practical Obscurity,'* A Paper Presented to TPRC: The 29th Annual Conference on Information Communication and Internet Policy, Oct. 27-29, 2001, TPRC-2001-096 citing 60 lower court decision on practical obscurity and FOIA; Arminda Bradford Bepko, *Public Availability or Practical Obscurity: The Debate Over Public Access to Court Records on the Internet*, 49 N.Y. Law School Law Review, p. 967 discussing the application of practical obscurity to federal and state court policy.

7 Center for Democracy and Technology, *Congress Hurries to Limit Public Right to Know,* CDT Policy Post Vol. 5, No.9, May 20, 1999, available at http://www.cdt.org/publications/pp_5.9.html.

8 Linda-Jo Schierow, *Accident Prevention under the Clean Air Act Section 112(r): Risk Management Planning by Propane Users and Internet Access to Worst-Case Accident Scenarios*, CRS RL30228, June 10, 1999, available at http://www.opencrs.com/document/RL30228/.

9 The probable futility of such policies has been raised in theory for years. *See supra* Davis, TPRC 2001-096 and CDT Policy Post Vol. 5, No 9.

cally obscure and making it easily accessible to the public on the Internet.

II. Three Examples of the Increasing Futility of Practical Obscurity

There are many examples of government information that was once practically obscure, but has since been made widely available by non-governmental actors. Some of these were originally obscured as part of specific policy decisions to try to obscure non-classified and non-confidential data. Other data have been obscured, not through active policymaking or law, but by the fact that most of the records are in paper or legacy databases not readily available to the broader public. I will focus on three of these cases.

A. Chemical Risk Management Plans

As discussed above, when the U.S. Congress passed a law to limit access to chemical plant risk management plans, it decreed that access to this public information should be provided to the public only through the federal depository libraries. This decision was made in part because it was clear from the Emergency Planning and Community Right-to-Know Act of 1986 that the Toxic Release Inventory Information, of which the RMPs are a part, was collected with publication in mind, so that local officials and even the media could examine the risk of local plants and create emergency plans.[10] Several environmental and right-to-know advocacy groups, led by OMB Watch, believed that the government's decision was made more in deference to the desires of the chemical industry than out of any sort of balanced policy-making process. These groups decided to systematically gather RMP summaries from the depository libraries and use them to create their own database.[11] Today, anyone can get access to these plans on the Web despite Congress' attempt to obscure them.

10 *See* Title III of PL 99-499.

11 OMB Watch, "Access to Government Information Post 9/11" Feb. 1, 2007, available at http://www.ombwatch.org/article/articleview/213/1/1.

B. CRS Reports

The Congressional Research Service (CRS) is a division of the Library of Congress that taxpayers pay $100 million a year to support. CRS serves as a kind of think tank for Congress providing unbiased, nonpartisan research on the key issues facing the country.[12] As part of its duties, CRS attempts to address questions that will be of interest to a wide range of members of Congress and their staff. These reports are then made available on an internal Web site available only to Capitol Hill offices.[13] Because these reports are non-classified and non-confidential, Members of Congress are free to distribute them to their constituents in paper or electronic form. In this case, the policy of practical obscurity appears to be intended to protect the unique relationship that CRS has with Congress. However, some private companies have found a means to collect all of the reports as they are posted and sell them for as much as $20 a piece on the Internet, so the reports are being made available to those that can afford them.[14] Access advocates, including Members of Congress,[15]

12 *See* http://www.opencrs.com/about.php.

13 Http://www.crs.gov redirects a user off of Capitol Hill to a the CRS Employment Opportunities Page, but sends a user with a Capitol Hill assigned Internet Protocol address to the CRS website.

14 LexisNexis provides CRS reports as part of its Congressional service package at http://www.lexisnexis.com/help/cu/CU.htm#TP/CRS_Reports.htm, or back reports in bulk at different prices http://www.lexisnexis.com/academic/catalog/2006intl_pdfs/UPA_Collections_CongressionalResearchService.pdf; Penny Hill Press Sells individual reports as its main business model at http://www.pennyhill.com/; Roll Call's Gallery Watch also resells Penny Hill's reports at http://www.gallerywatch.com/m_news-press.htm.
3) CQ sells access to CRS reports as the lead item in their "Top Docs" Product at http://www.cq.com/corp/show.do?page=products_cqtopdocs.

15 "All of these reports are 'public' for only those who can afford to hire a lawyer or lobbyists, or who can afford to physically travel to Washington to visit the Office of Public Records. That is not very 'public,' and does almost nothing for the average citizen in Vermont or the rest of this country who does not have easy access to Washington." Senator Patrick Leahy (D-VT), available at http://leahy.senate.gov/

have long asserted that Congress should make these documents available to the public directly and have been especially outraged to see them being sold.[16]

Several public interest groups and libraries[17] have created collections of reports in their respective issue areas and, in 2005, the Center for Democracy and Technology (CDT) created the OpenCRS web site[18] to tie these different collections together and make them widely available. OpenCRS has taken advantage of the decentralized nature of the Internet by establishing a single interface that allows citizens to easily peruse and download reports from a large and growing network of available CRS collections. The site also encourages users to grow the database, by uploading copies of any new CRS reports they happen to obtain on their own. While OpenCRS does not have every non-classified and non-confidential CRS report, the site and the sale of all of the reports has generally rendered the policy of practical obscurity useless since anyone with means can obtain the reports.[19]

C. Court Records

The openness of judicial proceedings has always been a fundamental principle of the court systems in the United States. However, the courts are facing some unexpected consequences of that openness as they become increasingly reliant upon the Internet. With caseloads growing each year, the Internet has become a valuable tool for court officials in terms of managing cases in an efficient and timely manner and streamlining document processing. At the same time, courts are using the Internet to give the public electronic access to court records, making judicial proceedings more transparent and making access more equitable,[20] but also making widely available personally identifiable and sometimes sensitive information that used to be practically obscure.[21]

For several years, advocates have suggested that increased posting with no changes to current policy could lead to identity theft using those records.[22] Recently, those predictions have proven to be prescient. In one harrowing case, a methamphetamine addict seeking to commit identity theft was found using local divorce records "listing the parties' names, addresses and bank account numbers, along with scans of their signatures. . . . all he needed to print checks in his victims' names."[23]

press/200302/021103a.html.

16 In a 1998 report, CDT and OMB Watch placed CRS reports as the number one "most wanted" set of government documents, available at http://www.cdt.org/righttoknow/10mostwanted/.

17 These groups include National Council for Science and the Environment, Federation of American Scientists, Thurgood Marshall Law Library/University of Maryland School of Law, National Memorial Institute for the Prevention of Terrorism, and Center for Democracy & Technology.

18 http://www.opencrs.com.

19 According to Jill Brett, from the Library of Congress, "If [the CDT] can get the reports and put them up, we can't stop them." Brian Faler, *Hard-to-Get Policy Briefings For Congress Are Now Online: Technology Group Opens Access to Research Reports,* Wash. Post, June 28, 2005, at p. A-13.

20 Companies such as ChoicePoint, LexisNexis and West Publishing have been charging for access to digitized court records for years.

21 *See* Center for Democracy and Technology, *A Quiet Revolution in the Courts: Electronic Access to States Court Records—A CDT Survey of State Activity and Comments on Privacy, Cost and Accountability Issues*, Aug. 2002, available at http://www.cdt.org/publications/020821courtrecords.shtml.

22 For example, "[T]he crime of identity theft will be fueled by easy access to personal identifiers and other personal information via electronic public records," Beth Givens, Director, Privacy Rights Clearinghouse, *Public Records on the Internet: The Privacy Dilemma*, Computers Freedom and Privacy Conference, Apr. 2002. Available at http://www.cfp2002.org/proceedings/proceedings/givens.pdf.

23 John Leland & Tom Zeller, *Technology and Easy Credit Give Identity Thieves An Edge*, N.Y. Times, May 30, 2006, at A1. Prior to this case, most experts cited the FTC and GAO reporting on identity theft showing that 61.7% of identity theft victims simply did not know who the thief was and those that did knew the thief, *see* Government Accountability Office, *Identity Theft: Prevalence and Cost Appear to Be Growing*, Mar. 2002, GAO-02-363, available at http://www.gao.gov/new.items/d02363.pdf (suggesting that the threat from public records was theoretical).

Several committees and groups have been formed by state and federal have made attempts to provide guidance on the privacy issues raised by placing previously practically obscure documents directly online.[24] These guidance documents have been helpful in setting broad policy but, as seen in the Arizona case, have not solved the problem completely.

III. Overview of Broad Access Policy Alternatives in the Internet Age

Looking over existing laws, legislation and discussions in the areas of information policy, one can identify five groupings of policies:[25]

1) **Open Access**—In this approach, governments provide the broadest access to public records by placing them on the Internet, unmodified from their current paper or electronic format. This maximizes access but does not address privacy and security issues.

2) **No Access**—Under this policy, government does not place any public records that may be potentially sensitive online. Officials could comb through information that is already available both in paper and online and prevent access. This minimizes access, but maximizes privacy.

3) **Enhancing Practical Obscurity**—This update to the old system is a planned version of the practical obscurity defined by the court. Government creates a bifurcated records system that would limit online access to certain private or sensitive information, but leave the complete paper or electronic record available for public review at the record holder's office. This is often held up as a middle ground approach.

4) **Use limitations—**A very common approach is to provide broad access for certain pre-defined purposes set forth in law or policy, and to restrict access for all other purposes.

5) **Review and Redact**—Under this policy, governments review the collection policies for public record-keeping and modify them to protect individual privacy or security interests.

III. Reaching a Balanced Policy

None of the above policy choices is perfect. Public information varies widely, as do the situational dynamics associated with specific data sets. There are several factors that come into play in making determinations about what may be the best policy for a particular situation, government agency or data set. These considerations include but are not limited to: the type of data and its potential benefit in being made widely available versus its potential harm; the resources of the agency posting the data; and historical use and access to the data. With these potential considerations in mind, policymakers can think through the options in Section II.

To begin with, we should remove the first two approaches (open access and no access) from con-

24 Several states have also had their own advisory committees. I was a member of the Maryland Committee on Access to Court Records in 2001 (*see* http://www.courts.state.md.us/access/index.html, conclusions and other information) and other states have had similar groups including Washington and New York. *See* Martha Wade Steketee & Alan Carlson, *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts,* Nat'l Center for State Courts & the Justice Management Institute, Oct. 2003, available at http://www.ncsconline.org/WC/Publications/Res_PriPub_GuidelinesPublicAccessPub.pdf.

25 *See* Sol Bermann's instructive paper, *Privacy and Access to Public Records in the Digital Age*, Center for Interdisciplinary Public Law & Legal Theory Working Paper Series No. 62, Law and Policy Studies Working Paper Series No. 40, Apr. 2006, focus suggests four of these same policy options. I have reordered them and added "Use limitations," but we come to similar conclusions on the problem and potential solutions.

sideration simply because they suggest an easy answer to a difficult problem. Proponents of each extreme suggest that one basic tenet of American society—government and corporate accountability, efficiency and openness; security and/or privacy must trump the other. Pollsters usually like to take what are really four concerns (government accountability, privacy, security, and government efficiency) and offer only two binary options: you can either have privacy or security; or you can either have security or efficiency.[26] Yet, when given multiple options, poll results clearly suggest that Americans do not want to sacrifice one of these tenets over another.[27] In fact, they expect government to be able to find a way to protect privacy and security in a way that does not detract from government accountability or efficiency. As such, striking this proper balance should be the goal of any policy designed to address these difficult policy challenges.

The next approach, enhancing practical obscurity, seems reasonable in its framing. Proponents simply want to modernize the current system. The major difference is that, whereas the Supreme Court treated practical obscurity as a kind of happy accident, using—or purposely not using—technology to help obscure information raises entirely different issues. In brief, the problem with this policy, as we have seen with the Chemical Plant Risk Model Plans and CRS Reports, is that in an age of inexpensive storage of information,[28] inexpensive imaging equipment, powerful optical character recognition software, and increasingly powerful database software it is very difficult, if not impossible, to keep public documents practically obscure. In fact, there is a clear policy advantage to the government in posting public materials online themselves, because they can generally control the context in which they are made available.

The fourth option—use limitations—has become more common to enhance privacy protections by limiting the use of information usually by placing strong restrictions and then creating exceptions for particular uses. For example, in 1994, the U.S. Congress passed the Driver's Privacy Protection Act (DPPA).[29] The DPPA prevents state governments from selling driver and identity card information without the consent of the individual. Yet, the statute has many exemptions including:

> For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors.[30]

In other words, businesses can obtain driver information for the broad purpose of fraud prevention. Exceptions have caused states such as North Carolina to pass even stronger laws that require the written consent of the individual for some information.[31] The key to this policy is that it restricts subsequent use and onward transfer of the information. Whereas enhanced practical obscurity policies simply place limitations on the original use of information, use limitations allow the flexibility to limit future uses as well.

26 For example, in May 2006, ABC News and the Washington Post conducted a poll asking for a binary choice, "What do you think is more important right now -- for the federal government to investigate possible terrorist threats, even if that intrudes on personal privacy; or for the federal government not to intrude on personal privacy, even if that limits its ability to investigate possible terrorist threats?" Available at http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_nsa_051206.htm.

27 The Council for Excellence in Government, "The New e-Government Equation: Ease, Engagement, Privacy and Protection," Apr. 2003. Available at http://www.excelgov.org/admin/FormManager/filesuploading/egovpoll2003.pdf.

28 *See* Ari Schwartz *et.al.*, *Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues*, 1 ISJLP 597, Summer 2005, for other examples of the policy impact of cheap storage.

29 18 U.S.C. § 2721.

30 18 U.S.C. § 2721(b)3.

31 North Carolina has detailed information about the program, including consent forms, on their website available at http://www.ncdot.org/dmv/other_services/recordsstatistics/copyDrivingRec.html.

Some states have attempted to combine a use limitation policy with an enhanced practical obscurity policy. For example, data brokers that provide access to voter registration information cannot provide Pennsylvania or South Dakota information over the Internet and cannot even take orders for Arizona voter lists online.[32] It seems clear that the states in these cases are attempting to limit the wide distribution of the material and allow most other uses. Unfortunately, they appear only to be creating a speed bump since data brokers are still selling this information in paper format that can be scanned and easily put into databases.

The major problem with use limitation laws is that they are in clear conflict with the fundamental openness tenet that government should not be able to control how non-classified government information is used. Also, if not crafted carefully, such policies can be so vague as to be easily abused[33] and can also run afoul of the principles of free expression.[34] Policymakers must consider all current and potential uses in order to create policies that are neither so restrictive that legitimate uses are ignored, nor so lenient that the policy may as well not exist. Therefore, crafting a balanced use limitation policy will always be a complicated endeavor fraught with potential unintended consequences.

The final policy alternative, review and redact, allows for broad access to a base set of information but attempts to safeguard privacy and security by limiting access to the most concerning pieces of data. This approach has become more common. In some recent examples:

- The federal government has encouraged agencies to stop using Social Security Numbers in public records as identifiers to protect individuals from potential identity theft.[35]
- Federal bankruptcy courts have begun redacting bank account and social security information when publishing court documents.[36]
- Agencies that provide satellite-mapping data have blurred images only over sensitive buildings, such as embassies or military bases.[37]

32 The data broker company, Aristotle, explains on its web site, "Use of and access to voter list data is restricted in some jurisdictions. For information, contact an Aristotle representative. AZ voter data is not available on the Internet. Orders for PA & SD voter data may be placed; however, the data will be delivered separately as it is not available for download over the Internet. Searching for individual voters is not available, and voter names and addresses are not visible during your searches." Available at http://www.aristotle.com/index.php?option=com_content&task=view&id=31&Itemid=64

33 My favorite example of the abuse of a privacy exception was when the National Zoo declared a privacy exemption to the Freedom of Information Act when a reporter sought the medical records of the Zoo's Pandas. James V. Grimaldi, *National Zoo Cites Privacy Concerns in Its Refusal to Release Animal's Medical Records*, Wash. Post, May 6, 2002, p. E12. Aside from the fact that the privacy of animals has not been upheld by any court, the Zoo itself provides a service called "PandaCam" where web users can watch the panda's activities at all times. Available at http://nationalzoo.si.edu/Animals/GiantPandas/default.cfm.

34 These are complicated issues; especially when discussing the role of government in limiting use of information collected by government. For an interesting debate of the general issue of privacy and speech, *see* Eugene Volokh, *Freedom of Speech and Information Privacy*, 52 Stan. L. Rev. 1049 (2000); and Paul M. Schwartz, *Free Speech vs. Information Privacy*, 52 Stan. L. Rev. 1559 (2000).

35 OMB released a "plan to eliminate unnecessary use of Social Security Numbers" as part of a memo in July 2007, OMB Memo 07-19, available at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf. Technically speaking, non-congressionally approved uses of the social security number were outlawed by the Privacy Act of 1974, 5 U.S.C. § 552a.

36 There have been several projects on this issue had several projects including a set of guidance that came from a detailed U.S. Treasury Report, *Financial Privacy in Bankruptcy:* A Case Study on Privacy In Public and Judicial Records, available at http://www.ustreas.gov/press/releases/reports/bankrstudy.pdf.

37 Other governments have taken a more extreme approach of no access or strong use limitations to mapping data. Most recently *see* Dan Charles, "Security Officials Seek to Block Some Online Maps," National Public Radio, Oct. 10, 2007, available at http://www.npr.org/templates/story/story.php?storyId=15091682.

This approach clearly has the potential for the greatest balance between openness and competing values because it allows for a tailored approach. However, putting a review and redact policy in place is not nearly as easy as other policy approaches. Finding the right balance of what information should be included and what should be redacted can be complicated and contentious. Also, once a redact policy has been determined, locating all of the records that need to be redacted can be resource intensive even with the use of technology to help.

IV. Conclusions

Practical obscurity is now merely a remnant of an accidental policy that worked prior to the digital age. Unfortunately, there are no easy, one-size-fits-all policy answers to address the fundamental conflicts in making potentially sensitive government information widely available in a networked world. In fact, the two kinds of policies most likely to achieve a workable balance for competing policy aims are also the most difficult to implement. Achieving the best resolution takes a broad understanding of all competing needs and may also require substantial resources and skilled governmental facilitation to be properly implemented.

Policymakers faced with this challenge should begin by examining a possible review and redact approach. This will mean beginning a public consultation with all interested parties to examine the extent of the concerns with particular data sets. Policymakers must then determine whether such information can be placed online as a whole or only after it is scrubbed of specific pieces of information. Next, a technical discussion is needed to examine the potential difficulties associated with redacting a portion of a specific data set. For example, it is easy to say that Social Security Numbers and Bank Account information should be removed from court records, but, assuming that these numbers are embedded in court filings and not in a database, finding these identifiers can be a difficult task. Once the scope of the project is determined, a final public consultation should be held to ensure that the process has addressed concerns.

If such a process is simply not possible, then the more difficult but possibly less resource-intensive task of placing use limitations on certain data sets should be examined. As mentioned above, the goal should be to achieve a balanced policy that is not so restrictive that it stops legitimate use of government information, but is still strong enough to mitigate potential security and privacy vulnerabilities.

Finally, it is important to note that considerations of what should be available online should not only focus on what is currently public. Policymakers that are examining the issue of what government information should and should not be available online should take a broader view and examine all information held, not just that which has been made public in the past. Without a regular examination of what can be made available and how it should be made available, the public may be missing out on potentially valuable information and the government will rightfully be seen as merely trying to obscure information rather than embrace openness.

4.2 Homeland Security v. Homeland Defense: Gaps Galore

by Jody R. Westby[38]

Introduction

Since the formation of the President's Commission on Critical Infrastructure Protection in 1996, sig-

38 Jody R. Westby is CEO of Global Cyber Risk LLC in Washington, D.C. and serves as Adjunct Distinguished Fellow to Carnegie Mellon CyLab. She chairs the American Bar Association's Privacy & Computer Crime Committee (Section of Science & Technology Law) and is a member of the World Federation of Scientists' Permanent Monitoring Panel on Information Security. She represents the ABA on the National Conference of Lawyers and Scientists.

nificant work has been undertaken by U.S. agencies and departments and state and local governments with respect to the protection of critical infrastructure (CI) and public-private sector coordination in the event of a cyber attack. The associated legal and policy issues have also been reviewed and actions have been taken to ensure an appropriate legal framework is in place to support Homeland Security response measures.[39] *Little has been done, however, with respect to (a) public-private sector response coordination in a cyber warfare context, and (b) the development of domestic and international legal and policy frameworks to support such responses*. Thus, there are significant preparedness gaps between the Homeland Security capabilities exercised by infrastructure owners and local, state, and federal responders and the Homeland Defense capabilities required from the U.S. military and other nation states. It is precisely these Homeland Defense gaps that leave America most vulnerable. In the post-9/11 world, responses to major cyber attacks will require (a) enormous interaction and cooperation between the public and private sectors, (b) clear legal authority for actions taken by the U.S. military and any collective assistance from other nation states, and (c) authorization from private sector boards of directors and senior management regarding the use of private sector networks in offensive and defensive actions.

Definitions and context are important when discussing Homeland Security, Homeland Defense, and critical infrastructure protection, and when analyzing the legal instruments that govern potential responses by nation states to cyber attacks. For purposes of this paper, "Homeland Security" is defined as "[a] concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[40] "Homeland Defense" is defined as "[t]he protection of United States territory, sovereignty, domestic population and critical infrastructure through deterrence of and defense against direct attacks as well as the management of the consequences of such attacks."[41] Section 2 of the U.S. Homeland Security Act defines "critical infrastructure" as having the same meaning as that used in the USA PATRIOT Act:

> [T]he term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the . . . [nation] that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[42]

39 *See e.g., Adequacy of Criminal Law and Procedure (Cyber): A Legal Foundations Study*, President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=184; *Approaches to Cyber Intrusion Response: A Legal Foundations Study*, 1997, President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=190; *Federal Government Model Performance: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=189; *Legal Authorities Database: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=181; *Legal Foundations, Studies and Conclusions: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=167; *Legal Impediments to Information Sharing: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=188; *Liability and Insurance: Infrastructure Assurance,* President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=168; *Major Federal Legislation: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=179; Ethan B. Kapstein, *Regulating the Internet*, President's Commission on Critical Infrastructure Protection, 1997, available at http://chnm.gmu.edu/cipdigitalarchive/object.php?id=170.

40 *National Strategy for Homeland Security,* Office of Homeland Security, July 2002 at 2, available at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

41 General Military Training – Homeland Defense, available at https://www.cnet.navy.mil/cnet/gmt/gmt03/1_5.pdf.

42 Homeland Security Act of 2002, Pub. Law 107-296,

The Threat

The threat of cyber warfare is not new. In fact, the U.S. Government has exercised cyber warfare tactics probably more than any other nation. Two excellent examples of U.S. cyberwar tactics are Operation Desert Storm and a successful CIA plot to disrupt Soviet pipelines. In 1982, President Reagan approved a plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union that had embedded features designed to cause pump speeds and valve settings to malfunction. "The result was the most monumental non-nuclear explosion and fire ever seen from space," noted former Air Force Secretary Thomas C. Reed in his book, *At the Abyss: An Insider's History of the Cold War.*"[43] The attack caused enormous economic and psychological impact to the Soviet Union and is credited with helping to end the Cold War.[44] The U.S. deployed cyber warfare tactics again when it invaded Iraq in 1991. Phase I of Operation Desert Storm was a strategic air campaign that would "attack Iraq's strategic air defenses; aircraft/airfields; …command and control systems; … telecommunications facilities; and key elements of the national infrastructure, such as critical … electric grids…."[45] The U.S. also used its extensive communication and satellite systems to support its Desert Storm activities.[46]

The U.S. is not alone in developing cyber warfare tactics and strategies. As early as 1996, U.S. Government officials estimated that more than 120 countries either had or were developing computer attack capabilities that could enable them to take over the Department of Defense's (DoD) information systems and "seriously degrade the nation's ability to deploy and sustain military forces."[47] Considering that today over one billion online users[48] and 233 countries are connected to the Internet,[49] the number of countries with such capabilities is likely higher.

China has long been considered one of the more aggressive countries focusing on cyber warfare capabilities, but speculation in this area was clarified when *Xinhua* published the full text of China's *National Defense in 2006*. In this document, China declared its goal of "building informationized armed forces and being capable of winning informationized wars by the mid-21st century."[50] The U.S.-China Economic and Security Review Commission (USCC) noted in its 2006 annual report to Congress that:

> Chinese military strategists write openly about exploiting the vulnerabilities created by the U.S. military's reliance on advanced technologies and an extensive C4ISR infrastructure it uses to conduct operations. China's approach to exploit-

Section 2, available at http://whitehouse.gov/deptofhomeland/bill. The USA PATRIOT Act is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

43 David E. Hoffman, "CIA slipped bugs to Soviets," *Washington Post,* Feb. 27, 2004, available at http://www.msnbc.msn.com/id/4394002.

44 *Id.*

45 *Operation Desert Storm: Evaluation of the Air Campaign,* U.S. Government Accountability Office, Letter Report, GAO/NSIAD-97-134, June 12, 1997 at Appendix V, available at http://www.fas.org/man/gao/nsiad97134/app_05.htm.

46 Jon Trux, "Desert Storm: A space-age war," *NewScientist,* July 27, 1991, available at http://www.newscientist.com/article/mg13117794.900-desert-storm-a-spaceage-war--one-year-ago-next-week-iraqinvaded-kuwait-provoking-a-war-with-the-us-and-its-allies-but-withoutanarmada-of-snooping-satellites-iraqs-battle-was-lost-almost-before-it-began.html.

47 *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* United States Gov't. Accountability Office, GAO/AIMD-96-84, May 22, 1996, available at http://www.fas.org/irp/gao/aim96084.htm.

48 "Internet Usage Statistics – The Big Picture: World Internet Users and Population Stats," Internet World Stats, available at http://internetworldstats.com/stats.htm (hereinafter "Internet Usage Statistics").

49 "Internet World Stats: Usage and Populations Statistics," available at http://www.internetworldstats.com/.

50 "China's National Defense in 2006," *Xinhua,* Dec, 29, 2006 at 5, available at http://news.xinhuanet.com/english/2006-12/29/content_5547029.htm.

> ing the technological vulnerabilities of adversaries extends beyond destroying or crippling military targets. Chinese military writings refer to attacking key civilian targets such as financial systems…. According to the Department of Defense, the PLA's [People's Liberation Army] cyber-warfare strategy has evolved from defending its own computer networks to attacking the networks of its adversaries and limiting their ability to obtain and process information….Such attacks would be intended to disable defense systems that facilitate command and control and intelligence communication and the delivery of precision weapons, primary instruments for the conduct of modern U.S. warfare.[51]

The USCC's 2007 report to Congress expanded on its earlier warnings by noting that a Chinese cyber attack might go beyond government systems and target U.S. financial, economic, energy, and communications infrastructure.[52]

In June 2007, Pentagon computer networks were allegedly hacked by the Chinese military in what has been called "the most successful cyber attack on the U.S. defense department,"[53] shutting down parts of the Pentagon's systems for more than a week.[54] Chinese hackers have also been blamed for attacks that compromised German government systems and cyber espionage incidents against the United Kingdom's (UK) government systems.[55] The Director-General of the UK's counter-intelligence and security agency, MI5, recently posted a confidential letter to 300 CEOs and security officers on the website of the Centre for the Protection of National Infrastructure, warning them that their infrastructure was being targeted by "Chinese state organizations" and that the attacks were designed to defeat security best practices.[56]

Cyber threats do not emanate solely from nation states, however. Government officials have repeatedly warned that terrorists or other rogue actors have the capability to attack critical infrastructure and cause catastrophic consequences. Analysis of the use of the Internet and information and communication technologies (ICTs) by terrorists confirms their interest in and ability to use these technologies for asymmetric attacks. For example, after September 11, the U.S. Federal Bureau of Investigation (FBI) discovered that online users, whose activity was routed through switches in Saudi Arabia, Pakistan, and Indonesia, were exploring the digital systems of emergency telephone, electrical generation and transmission, water storage and distribution, nuclear power plants, and gas facilities.[57] Computers seized in Pakistan in July 2005 contained material from "casings" of key financial institutions located in New York, Washington, D.C., and Newark, New Jersey, prompting Homeland Security alerts to these organizations and locales.[58]

---

51 *2006 Report to Congress of the U.S.-China Economic and Security Review Commission*, Nov. 2006 at 137, available at http://www.uscc.gov/annual_report/2006/06_annual_report_contents.php. C4ISR is an acronym for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

52 *2007 Report to Congress of the U.S.-China Economic and Security Review Commission*, June 1, 2007 at 8, available at http://www.uscc.gov/annual_report/2007/annual_report_full_07.pdf.

53 Demetri Sevastopulo, "China 'hacked' into Pentagon defence system," *Financial Times,* Sept. 6, 2007 at 1.

54 Demetri Sevastopulo, "Real security fear over virtual invasions," *Financial Times,* Sept. 4, 2007 at 2.

55 "China's cyber-spies spread their net," *Financial Times,* Sept. 4, 2007 at 12; Andrew Ward and Demetri Sevastopulo, "US concedes danger of cyber-attack," *Financial Times,* Sept. 6, 2007 at 3.

56 Rhys Blakely, "MI5 alert on China's cyberspace spy threat," *Times Online,* Dec. 1, 2007, available at http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece.

57 Jody R. Westby, "Countering Terrorism with Cyber Security," *Jurimetrics,* Vol. 47, No. 3, Spring 2007 at 297, 306-307, available at http://lawlib.wlu.edu/CLJC/index.aspx?mainid=163&issuedate=2007-09-12&homepage=no (hereinafter "Westby") (citing Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 26, 2002, available at http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26).

58 Westby at 306-307 (citing "Al-Qaeda surveillance

The Need for Response Coordination

Cyber response capabilities must be closely coordinated because, at the time of a cyber attack, it is not possible to immediately determine whether the attacker is a script kiddie, an insider, a rogue actor (organized crime, terrorist organization, or radical), or a nation state. Therefore, the "response baton" may have to be passed from the private sector to law enforcement to the military with swift, efficient coordination and certainty regarding legal authority for actions taken.

It is imperative that cyber response capabilities be analyzed from the perspective of cyber warfare and/or attacks from terrorists, including public-private sector coordination and the information sharing that will be required to shift from local responders to military involvement. Unlike traditional defense categories (i.e., land, air, and sea), the military capabilities required to respond to an attack on U.S. infrastructure will necessarily involve infrastructure owned and operated by the private sector. Indeed, 85 percent of CI in the U.S. is owned by the private sector.[59] What is more, the Department of Defense (DoD) is critically dependent upon these infrastructures, both domestically and globally, to support its operations. A 1995 research report to the Joint Chiefs of Staff noted that "over 95 percent of the worldwide telecommunications needs of the Department of Defense (DoD) are satisfied by commercial telecommunications carriers."[60] Thus, the very networks that support DoD operations and network-centric warfare capabilities – including defensive and offensive cyber capabilities – are not under the direct control of DoD and require private sector involvement for offensive and defensive capabilities.

The military has long embraced the concept of information operations and has developed extensive materials in the area of cyber warfare.[61] In 2005, the Joint Functional Component Command for Network Warfare (JFCCNW) was established to "facilitate cooperative engagement with other national entities in computer network defense and offensive information warfare."[62] The JFCCNW is headed by the director of the National Security Agency (NSA), presently Lt. General Keith B. Alexander, but it is a component of the United States Strategic Command (STRATCOM), which coordinates offensive computer network operations for DoD.[63] The establishment of the JFCCNW is a critical step toward creating a formal cyber defense category and response capability.

Since its establishment, however, the JFCCNW has done little to reach out to the private sector to plan their involvement – and the use of their networks – in the cyberwar offensive and defensive actions. The deployment of military weapons is traditionally under the complete control of the U.S. President as Commander and Chief of the Armed Forces and the Department of Defense.

techniques detailed," *USA Today,* Dec. 29, 2004, available at http://www.usatoday.com/news/washington/2004-12-29-terror-surveillance_x.htm).

59 *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics,* Government Accountability Office, GAO-07-39, Oct. 2006 at 1, available at http://www.gao.gov/new.items/d0739.pdf.

60 Science Applications International Corp., *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance,* A Research Report for the: Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington, D.C. July 4, 1995 at 1-1, available at http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA316285&Location=U2&doc=GetTRDoc.pdf.

61 *See, e.g.,* Cyberspace & Information Operations Study Center, Air University, U.S. Air Force, available at http://www.au.af.mil/info-ops/; Naval Information Warfare Activity, available at http://www.fas.org/irp/agency/navsecgru/niwa/; U.S. Army Training and Doctrine Command, *Concept for Information Operations*, Aug. 1, 1995, available at http://www.tradoc.army.mil/tpubs/pams/p525-69.htm.

62 Statement of Gen. James E. Cartwright, Commander, United States Strategic Command, Before the Strategic Forces Subcommittee on Space Policy, Mar. 16, 2005 at 12, available at http://www.globalsecurity.org/space/library/congress/2005_h/050316-cartwright.pdf.

63 Joint Functional Component Command for Network Warfare, available at http://en.wikipedia.org/wiki/Joint_Functional_Component_Command_for_Network_Warfare.

Perhaps the notion that a cyber defense category and response capability involves private sector participation is foreign to military planning, but there is an urgent need for the JFCCNW to engage the private sector in offensive planning and the development of coordinated response capabilities in the event of cyber warfare.

The establishment of a cyber defense category and cyber response capability within DoD can only be effective – and considered within our correlation of forces – if it includes the coordination and cooperation of the private sector that owns and operates the very networks at risk and which would be used to launch an attack or counter-attack.

Quite simply, effective cyber actions require open channels of communication between the military and critical infrastructure owners, with scenarios and interactions well thought-out and rehearsed. These actions are a giant step beyond the Homeland Security efforts voluntarily undertaken by U.S. companies on an industry-sector basis to develop CI plans and establish information sharing and analysis centers (ISACs). This work has been undertaken in concert with a Government department or agency as the industry sector's public sector counterpart, as designated by Homeland Security Presidential Directive No. 7 (HSPD-7). HSPD-7 instructs each Government Sector-Specific Agency to "collaborate with … the private sector, including key persons and entities in their infrastructure sector."[64] HSPD-7 designates DoD as the Sector-Specific Agency (SSA)[65] for the defense industrial base (DIB).

HSPD-7 is implemented in DoD through Department of Defense Directive 3020.40 (DD 3020.40), which incorporates the collaboration requirement in the Directive's Purpose. DD3020.40 defines Defense Critical Infrastructure as "DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide."[66] DD3020.40 defines the Defense Industrial Base (DIB) Defense Sector as "[t]he Department of Defense, the U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements."[67] Notably, this definition excludes the private sector entities that DoD would have to rely upon for cyber warfare offensive and defensive actions. In fact, the *Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan* specifically notes that:

> The DIB *does not* include commercial infrastructure that provides, for example, power, communications, transportation, and other utilities that DoD warfighters and support organizations use to meet their respective operational needs. Those commercial infrastructures are addressed by the other SSAs and through dependency analysis.[68]

To date, DoD's interactions with the private sector have largely been limited to working with defense industrial base companies to secure their information technology systems to protect information regarding U.S. weapons systems and DoD data. Efforts to work more broadly with the private sector on defining roles and responsibilities in cyber warfare offensive and defensive situations have

64 Homeland Security Presidential Directive / HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection, Dec. 17, 2003 at 4, available at http://www.fas.org/irp/offdocs/nspd/hspd-7.html.

65 *Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* U.S. Department of Defense, May 2007 at 5, available at http://www.dhs.gov/xlibrary/assets/DIB_SSP_5_21_07.pdf (hereinafter "DIB Plan").

66 Department of Defense Directive, "Defense Critical Infrastructure Program (DCIP)", No. 3020.40, Aug. 19, 2005 at 2, available at http://www.fas.org/irp/doddir/dod/d3020_40.pdf.

67 *Id.* at 11.

68 DIB at 5 (emphasis added).

not occurred, yet somehow DoD conveys the message that the U.S. is prepared for such actions.

General Cartwright, former commander of STRATCOM, aroused attention in his March 21, 2007 testimony before the House Armed Services Subcommittee by declaring that the best defense to cyber attacks against U.S. military, civilian, and commercial networks was a good offense:

> [If] we apply the principle of warfare to the cyber domain, as we do to sea, air and land, we realize the defense of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary, to deter actions detrimental to our interests.[69]

The General's comments are unhinged from the reality of private sector ownership of the critical infrastructure that must be used to launch an offensive attack and DoD's lack of interactions with the private sector on planning such attacks. *Indeed, with the exception of historic interactions with the communications sector through the National Communications Coordinating Center and the National Security Telecommunications Advisory Committee, DoD and the JFCCNW has not reached out to private sector entities to plan and coordinate cyber offensive and defensive actions*. Likewise, although CI owners have developed sector-specific plans for CI protection, they have not (a) adequately examined their role in responding to cyber warfare attacks on their infrastructure, (b) analyzed the legal considerations and risks that may be involved, and (c) developed response plans that involve coordination with the U.S. military and the involvement of their own personnel. In addition, neither the Government nor CI owners have adequately examined the interdependencies in critical infrastructure to begin developing response plans that support more than their own CI. *This gap between Homeland Security and Homeland Defense preparedness planning must be addressed immediately if the U.S. is to keep pace with the cyber warfare activities of other nation states and rogue actors and effectively execute offensive attacks and manage defensive response capabilities*. The recent attacks on government and private sector networks in Estonia demonstrate the rapid pace at which a cyber attack can escalate to a national security issue, involve other nation states, and raise the issue of collective defense. The Estonian attacks may also represent a situation in which rogue actors are aligned with a nation state in conducting and concealing such attacks, though this has not been proven. Serious cyber attacks, such as those directed at Estonia, cannot be countered by any private sector company; government assistance is necessary. These situations rapidly escalate beyond the capabilities of law enforcement, CERTs, and ISACs and military and cyber warfare expertise is required.

The attacks against Estonian government and private sector systems began April 26, 2007 and continued for several weeks. They involved hacking, web defacement, and sustained denial of service attacks that were amplified by the use of a large network of bots.[70] The attacks began after Estonian officials took down a popular bronze statue of a World War II Soviet soldier. They started with a flood of spam messages that eventually shut down the Estonian Parliament's email system. In another attack, hackers broke into the web site of the Reform Party and posted a phony letter from Estonia's prime minister apologizing for removing the statue. The attacks quickly escalated into what Estonia's defense minister called "a national security situation," seriously impacting government web sites and systems and shutting down

69 Bob Brewin, "Cybersecurity defense requires a good offense," *FCW.com,* Mar. 22, 2007, available at http://www.fcw.com/online/news/98016-1.html.

70 Bots are software robots that are planted in a computer by a hacker without the knowledge of the owner. They can be linked together into networks (called botnets) controlling millions of computers and can be activated remotely to perform automatic tasks, such as sending large packets of information. *See generally*, http://en.wikipedia.org/wiki/Internet_bot.

newspaper and financial networks.[71] The Estonian government was forced to close large parts of the country's network to outside traffic as it attempted to gain control of the situation. Estonia blames the attacks on Russia and claims that it has tracked some communications to an Internet address belonging to a Kremlin official.[72] Notably, Russia refused to cooperate in the investigation of the attacks even though it strongly denied any responsibility for them.[73] "They won't even pick up the phone," complained Rein Lang, Estonia's minister of justice regarding Russia's refusal to help end the attacks or investigate evidence that Russian state employees were behind them."[74]

The head of Estonia's Computer Emergency Response Team (CERT) initially summoned security experts from Estonia's Internet service providers (ISPs), financial institutions, government agencies, and police and called on contacts in other countries to help track and block suspicious Internet addresses and traffic. Before the attacks ended, computer security experts from the U.S., Israel, the European Union (EU), and the North Atlantic Treaty Organization (NATO) were assisting Estonia—and learning its lessons.[75] Traffic involved in the attacks was traced to countries as diverse as the U.S., China, Vietnam, Egypt, and Peru.[76] In a Joint Motion for a Resolution of the European Parliament, Estonia called on the European Commission and the Member States of the EU "to assist in the analyses of the cyber-attacks on Estonian websites and to present a study on how such attacks and threats can be addressed at the EU level. . . ."[77] Linton Wells II, then the principal Deputy Assistant Secretary of Defense for DoD networks and information integration, commented that "[t]his [the Estonian attacks] may well turn out to be a watershed in terms of widespread awareness of the vulnerability of modern society."[78]

Theory falls way to reality in the chaos that follows such crises: neither NATO nor the countries that came to the assistance of Estonia had clear legal authority to engage in defensive measures to aid Estonia. The Estonian attacks highlight the need to revise the doctrines and documents that traditionally support diplomatic, policy, and military decisions so they can accommodate cyber situations. The political and economic shifts caused by the Internet and globalization introduce geo-cyber considerations that impact more fundamental approaches to national security based on geo-political[79] interests and spheres of influence.

Geo-Cyber Considerations

On the heels of World War II, America was faced with a new kind of enemy: the Cold War, socialism, and threats of nuclear strikes. The Air Force became concerned about its ability to maintain command and control operations following a nuclear attack, and they commissioned RAND to

71 Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times,* May 29, 2007, available at http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&pagewanted=print&oref=slogin (hereinafter "Landler and Markoff").

72 *Id*.

73 David J. Smith, "Cyber-war!" *24 Saati*, Tblisi, Sept. 25, 2007, available at http://www.potomacinstitute.org/media/mediaclips/2007/Smith_24Hours_092507.pdf.

74 Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post,* May 19, 2007 at 1, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html (hereinafter "Finn").

75 Landler and Markoff.

76 Finn at A14.

77 Joint Motion for a Resolution, European Parliament, May 23, 2007 at 4, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+P6-RC-2007-0205+0+DOC+PDF+V0//EN.

78 Landler and Markoff.

79 Geopolitics is defined as "(1) The study of the relationship among politics and geography, demography, and economics, especially with respect to the foreign policy of a nation, (2)(a) A governmental policy employing geopolitics, (b) A Nazi doctrine holding that the geographic, economic, and political needs of Germany justified its invasion and seizure of other lands, (3) A combination of geographic and political factors relating to or influencing a nation or region." American Heritage Dictionary, 2000, available at http://dictionary.reference.com/search?r=2&q=geopolitical.

do a study on a survivable military network that could provide "minimum essential communications."[80] The RAND work (1962-1965) concluded with a report by Paul Baran describing how a packet switched computer network could provide this capability.[81] The rest is history. In 1971, the ARPANET, as the Internet was first called, had 23 hosts connecting government research centers and universities across the nation. In 1995, NSF turned access to the Internet backbone over to four commercial companies, and, by 1996, there were nearly 10 million hosts online and the Internet spanned the globe. Within three decades, the Internet grew "from a Cold War concept for controlling the tattered remains of a post-nuclear society to the Information Superhighway."[82]

Today, there are no U.S. Government controls or geographical boundaries on the Internet. Policies are determined by the Internet Society (ISOC) and other international bodies.[83] Since the NSF unleashed the Internet in 1995, it has experienced explosive growth, increasing from 50 million users in 1996 to around 1.2 billion today,[84] served by around 490 million hosts around the globe.[85] The negative repercussions to the Internet boom – viruses, worms, trojan horses, bots, network attacks, intrusions, web defacements, economic espionage, and interceptions of data are commonplace – also originate from all over the world, creating new threats and more closely linking national and economic security.

History repeats itself. Today, America once again faces new threats, and our ability to maintain our C4ISR capabilities against attacks from terrorists and nation states has become a national priority. September 11 changed our concept of national security, stood our military strategy on its head, and heightened our sensitivity to vulnerabilities in our critical infrastructure. We are faced with unprecedented asymmetrical challenges to our national and economic security. Although geo-political considerations still must be afforded great weight, threats to our critical infrastructure must be evaluated in a policy paradigm that is based on maintaining geo-cyber security and stability.

The author defines "geo-cyber" as the relationship between the Internet and the geography, demography, economy, and politics of a nation and its foreign policy. "Geo-cyber security" is defined as the ability to protect the infrastructure, systems, and information of a nation from intrusion, attack, espionage, sabotage, unauthorized access or disclosure, or other forms of negative or criminal activity that could undermine its national and economic security. "Geo-cyber stability" is defined as the ability to utilize the Internet for economic, political, and demographic benefit and to influence the policies, laws and regulations governing the Internet, while minimizing the risks and threats to economic and national security. [86]

Today, it is no longer a question of our maintaining "essential minimum communications;" it is a question of how we can maintain geo-cyber security so our critical infrastructure cannot be used as a weapon against us and how we can engage multilaterally to ensure geo-cyber stability. The irony is that the brainchild of the Cold War era now presents one of the most daunting challenges to Homeland Defense—one which we are ill-prepared to meet. Not only is there no planned co-

80 Dave Krisula, "The History of the Internet," Aug. 2001, available at http://www.davesite.com/webstation/net-history.shtml (hereinafter "Krisula"); "A Brief History of the Net," *Fortune*, Oct. 9, 2000 at 34; Stewart Brand, "Founding Father," *Wired*, Mar. 2001 at 148 (hereinafter "Brand").

81 Brand at 145-153; Krisula.

82 "Life on the Internet: Net Timeline," PBS, available at http://www.pbs.org/internet/timeline/timeline-txt.html; *see also* Krisula.

83 *See e.g.*, http://www.isoc.org/isoc/; http://www.wia.org/ISOC/.; http://www.iab.org/iab/.

84 Internet Usage Statistics.

85 Internet Systems Consortium, "ISC Domain Survey: Number of Internet Hosts," available at http://www.isc.org/index.pl?/ops/ds/host-count-history.php.

86 Jody R. Westby, "A Shift in Geo-Cyber Stability and Security," Paper presented at ANSER Institute of Homeland Security Conference, "Homeland Security 2005: Charting the Path Ahead," College Park, MD, May 6-7, 2002 at 2-3.

ordination for offensive and defensive cyber attacks, the legal framework to support such actions is murky at best.

Legal Issues

Numerous legal and policy questions arise in the context of cyber warfare. Consider how the U.S. might launch an offensive attack on China through communications infrastructure. DoD systems are not connected to China, so any attack would necessarily involve private sector networks. Who on the public and private sector sides would have authority to approve military use of private sector networks? What international cooperation would be required? Would the attack have to traverse more than one provider's network? Would allowing the use of the private network for military purposes interfere with the fiduciary duty owed to the company's shareholders by the board of directors and officers to protect company assets and its market value? Who is responsible for damage that could occur to the private sector network as a consequence of the attack or as the result of a counter-attack? Can the U.S. Government order a private sector company to let it take over its network for national security interests? What third party liability may arise as a result of such an attack?

Experts who have analyzed legal issues associated with cyber responses have noted that in kind cyber responses or active defense responses to cyber attacks could result in violations of domestic laws or, if the act is deemed to be a "use of force," it could violate the customary rules of war.[87] Other issues arise in the context of assistance from other countries, including multilateral assistance. The Estonian government quickly brought the cyber attacks on their systems to the EU and NATO, raising numerous questions regarding international law and prompting predictions that the attacks "will likely shape a debate inside many governments over how such attacks should be considered in the context of international law and what sort of response is appropriate."[88] "It was a concerted, well-organized attack, and that's why Estonia has taken it so seriously and so have we," noted Robert Pszczel, a NATO spokesman.[89]

Estonia's defense minister, Jaak Aaviksoo, pinpointed the gaps in the NATO treaty with respect to cyber attacks by stating:

> At present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country. Not a single NATO defense minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future."[90]

International cooperation is almost always needed in tracking and tracing cyber communications simply due to the interconnected nature of the Internet and the manner in which the Internet Protocol breaks a communication into packets and routes them across many networks before reassembling them at their destination point. Therefore, the cooperative efforts of nation states may also be necessary in defending against cyber attacks.

The two principal legal instruments that would govern multinational action in a cyber warfare situation are the NATO treaty and the United Nations (UN) Charter. Each document is more than 50 years old and their provisions do not accommodate cyber scenarios.

87 Thomas C. Wingfield, James B. Michael, Duminda Wijesekera, "Optimizing Lawful Responses to Cyber Intrusions," available at http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf.

88 Christopher Rhoades, "Estonia Gauges Best Response to Cyber Attack," *The Wall Street journal,* May 18, 2007 at A6.

89 Finn.

90 Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* May 17, 2007, available at http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

UN Charter

The United Nations defines aggression as "the use of armed force by a State against a sovereignty, territorial integrity, or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations…."[91]

The UN Charter has five articles that require scrutiny in the cyber warfare context: Article 2, paragraph 4, and Articles 41, 42, 51, and 99:

> Article 2
> 4. All Members shall refrain in their international relations from the threat or use of force **against the territorial integrity or political independence** of any state, or in any other manner inconsistent with the Purposes of the United Nations.[92]
>
> Article 41
> The Security Council may decide what measures not involving the **use of armed force** are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These **may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication**, and the severance of diplomatic relations.[93]
>
> Article 42
> Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it **may take such action by air, sea, or land forces** as may be necessary to maintain or restore international peace and security. **Such action may include demonstrations, blockade, and other operations by air, sea, or land forces** of the Members of the United Nations.[94]
>
> Article 51
> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an **armed attack** occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this **right of self-defense shall be immediately reported** to the Security Council….[95]
>
> Article 99
> The Secretary-General may bring to the attention of the Security Council any matter which in his opinion may threaten the **maintenance of international peace and security**.[96]

In analyzing these provisions, one first has to ask whether a cyber attack constitutes the use of force against the **territorial integrity or political independence** of another nation, as proscribed by Article 2. Although some cyber attacks that have the force to destroy communication networks (such as the Desert Storm attacks) might be deemed to harm the territorial integrity of a country, the general view is that they would not. Such attacks might well impact the political independence of a nation; however, if its government systems are shut down, web sites are defaced, and electronic government services are impaired. Would economic impact resulting from a cyber attack be considered the use

91 United Nations General Assembly Resolution 3314 (XXIX), Dec. 14, 1974, available at http://jurist.law.pitt.edu/3314.htm; *see also* Jeffrey F. Addicott, *Terrorism Law: Materials, Cases, Comments,* Lawyers & Judges Publishing Co., Inc., 4th ed., 2007 at 28 (hereinafter "Addicott").

92 Charter of the United Nations, Chapter I, Purposes and Principles, Article 2, para. 4, available at http://www.un.org/aboutun/charter/ (hereinafter UN Charter) (emphasis added).

93 UN Charter, Chapter VII, Article 41 (emphasis added).

94 UN Charter, Chapter VII, Article 42 (emphasis added).

95 UN Charter, Chapter VII, Article 51 (emphasis added).

96 UN Charter, Chapter XV, Article 99 (emphasis added).

of force against territorial integrity? Perhaps. The CIA plot to sell the Soviet Union bogus software that blew up its pipelines and wreaked significant economic harm to the country allegedly impacted the Soviet Union's territorial integrity by attributing to its downfall. It is a stretch, however, to fit cyber attacks within the meaning of Article 2.

Article 51 indicates that nothing shall block a nation or group of nations from engaging in collective self-defense if an **armed attack** occurs, raising the question of whether a cyber attack could be deemed to be an "armed attack." Even if the attack came from a branch of the armed forces, Article 41 cuts against this interpretation because it discusses **actions that may be taken that are *not* involving the use of armed force**. It specifically includes the complete or partial interruption of communications, which could encompass a cyber attack. Article 42 discusses actions that may be taken by **air, sea, or land forces, including blockades and "other operations.**" Cyber capabilities are well developed within the traditional air, land, and sea branches of the U.S. and foreign militaries. Could cyber military action by the Air Force, for example, that blocked traffic from a specific country or countries be considered an air attack or a blockade? Article 99 allows the Secretary-General to bring matters before the Security Council if **threaten international peace and security**. Would a cyber attack qualify as such a threat? If so, the Security Council could authorize actions by Member nations to block communications from one or more countries or to counter-attack under Article 42.

In sum, none of the UN Charter provisions neatly accommodate cyber attacks and provide clear legal authority for these types of events. The best course of action would be to amend the Charter to make it specifically address the geo-cyber security issues associated with cyber attacks and cyber warfare. It is also important that amendments to the UN Charter include the recognition that cyber defense categories and response capabilities constitute a legitimate branch of military forces alongside air, land, and sea. Chapter XVIII of the Charter governs amendments.

NATO Treaty

The North Atlantic Treaty (NATO Treaty) uses similar language as that in the UN Charter and is equally ambiguous regarding cyber attacks. In fact, Article 1 of the NATO Treaty requires the parties to "refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of the United Nations."[97] Traditionally, the term "act of war" "refers to the use of aggressive force against a sovereign State by another State in violation of the United Nations Charter and customary international law."[98] However, following the terrorist attacks on September 11, 2001, the North Atlantic Treaty Organization (NATO) invoked its collective defense clause, Article V, even though the attack came from a terrorist organization instead of a country.[99]

The five relevant provisions of the NATO treaty in the context of cyber attacks and cyber warfare are:

> Article 3
> In order more effectively to achieve the objectives of this Treaty, the Parties, **separately and jointly, by means of continuous and effective self-help and mutual aid**, will maintain and develop their individual and collective capacity to resist **armed attack**.[100]
>
> Article 4
> The Parties will consult together whenever, in the opinion of any of them, the

97 The North Atlantic Treaty, Article 1, North Atlantic Treaty Organization, Apr. 4, 1949, available at http://www.nato.int/docu/basictxt/treaty.htm (hereinafter "NATO Treaty").
98 Addicott at 23.
99 Addicott at 23.
100 NATO Treaty, Article 3 (emphasis added).

territorial integrity, political independence or security of any of the Parties is threatened.[101]

Article 5
The Parties agree that an **armed attack** against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[102]

Article 6(1)
For the purpose of Article 5, an **armed attack** on one or more of the Parties is deemed to include an armed attack:

- On the **territory** of any Parties….;
- On the **forces, vessels, or aircraft** of any of the Parties….[103]

Article 12
After the Treaty has been in force for ten years, or at any time thereafter, the Parties shall, if any of them so requests, consult together **for the purpose of reviewing the Treaty**, having regard for the **factors then affecting peace and security** in the North Atlantic area, including the development of universal as well as regional arrangements under the Charter of the United Nations for the maintenance of international peace and security.[104]

A review of the NATO Treaty leaves geo-cyber issues as unsettled as the UN Charter. Article 3 of the Treaty refers to self-help and mutual assistance, but only in the context of an **"armed attack."** Since the NATO Treaty is intended to be consistent with the UN Charter, it is unlikely that a cyber attack would be deemed to be an armed attack absent special circumstances, such as an attack using an electromagnetic pulse generation techniques.[105] The same issues with respect to **territorial integrity and political independence** arise under Article 4 of the Treaty as with Article 2 of the UN Charter. The addition of the words **"or security"** in Article 4, however, may open the door for consultation among NATO member states. Cyber attacks certainly raise national and economic security concerns since defense and financial networks are so dependent upon computer systems and connected networking capabilities. The central provision of the NATO Treaty is Article 5, calling for **collective assistance in the event of an "armed attack"** upon any Party to the Treaty. As the Estonian defense minister pointed out, NATO at this point would most likely not consider a cyber attack an armed attack for purposes of invoking an Article 5 collective response. This conclusion is further supported by Article 6(1) and its reference to **territory, forces, vessels, or aircraft** of any of the Parties. Article 12 does not authorize action but it does offer an avenue for reviewing the NATO Treaty in the context of cyber attacks and geo-cyber security and to include universal approaches and regional arrangements for responding to cyber events.

Upon examination of cyber attacks and the existing legal framework, the World Federation of Scientists' Permanent Monitoring Panel on Information Security supported the following conclusion in its report to the Secretary-General of the UN and the World Summit on the Information Society:

101 NATO Treaty, Article 4 (emphasis added).
102 NATO Treaty, Article 5 (emphasis added).
103 NATO Treaty, Article 6(1) (emphasis added).
104 NATO Treaty, Article 12 (emphasis added).

105 Carlo Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," available at http://www.globalsecurity.org/military/library/report/1996/apjemp.htm.

> As electronic information networks expand and military and industrial infrastructures become more dependent on them, cyber-attacks are bound to increase in frequency and magnitude. Interpretations of the UN Charter and of the laws of armed conflict will have to evolve accordingly in order to accommodate the novel definitions of the use of force that such attacks imply….
>
> In terms of the laws of armed conflict, the potentially dangerous consequences of an unnecessary response, a disproportional response or a mistakenly targeted response argue for keeping a human being in the decision loop.
>
> Beyond these preliminary conclusions, there is far more work to be done on both the international, technical, and legal fronts. Nations that choose to employ information operations, or that expect to be targeted by them, should facilitate tracking, attribution, and transnational enforcement through multilateral treaties and, more broadly, by clarifying international customary law regarding the use of force and self-defence in the context of the UN Charter and the laws of armed conflict.[106]

The need to update the legal instruments governing the actions of nation states with respect to cyber warfare and attack capabilities has never been more urgent. The rule of law is already in a precarious state due to the disruptions caused by terrorist activities. The ominous threat of cyber attacks by nation states and rogue actors can no longer be ignored. The UN Charter and NATO Treaty are antiquated and do not accommodate the electronic capabilities of the 21st century. Governments, the private sector, and multinational organizations must begin an international dialogue in this area to accommodate new military capabilities, collective action, and geo-cyber considerations.

Conclusion

There are gaps galore in our ability to counter cyber attacks and protect our critical infrastructure. There are gaps in ownership of weapons (i.e., the CI networks are owned by the private sector but would need to be deployed by the military in a cyber warfare situation). There are gaps in the response coordination that would be required to execute such attacks or defend the networks and gaps in defining responsibilities for command and control. There are gaps in the legal frameworks that would support such offensive, defensive, or collective cyber warfare actions. There are gaps in the prevailing policy mindset that would likely preclude effective decision-making: 20th century principals are not wholly adequate in the 21st cyber century.

The Internet has connected the globe and introduced new ways to harm national and economic security interests. It has also changed the traditional roles of the public and private sectors regarding national defense and public safety. Hard lines between law enforcement and military responsibilities are more blurred in the cyber context. An incident may look like an inside event at the outset but, upon investigation, require law enforcement assistance and, within short order, end up being a cyber attack by a nation state in concert with rogue actors.

The course ahead is clear. Military leaders must engage the private sector and develop offensive and defensive cyber response plans. CI owners must begin analyzing cyber warfare scenarios and mapping out response plans that will involve

106 Toward a Universal Order: Managing Threats From Cybercrime to Cyberwar. Report and Recommendations, World Federation of Scientists Permanent Monitoring Panel on Inforrmation Security, Nov. 19, 2003, World Summit on the Information Society, Document No. WSIS-03/GENEVA/CONTR/6-E, available at http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf (*citing* Grove, Goodman, and Lukasik at 100, available at http://survival.oupjournals.org/cgi/content/abstract/42/3/89).

military engagement and possibly coordination with other CI sectors. Legal experts, policy makers, and diplomats must work together to bring the legal instruments that underpin international peace and security into the electronic age. The urgency of the situation can hardly be overstated: without such action, we will face legal uncertainty and chaos when managing cyber attacks that are of such a nature that they can jeopardize public safety, national and economic security, global stability, and international peace. This is a risk we cannot afford to take.

4.3 Control System Cyber Security and Potential Legal Ramifications

by Joe Weiss, PE, CISM

Abstract

Industrial control systems such as Supervisory Control and Data Acquisition (SCADA), plant Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC) are used to monitor and control all types of industrial processes including production and distribution of electricity, water, oil, gas, chemicals, etc. These systems were designed with strict functional requirements such as reliability, availability, and time response. Originally, these systems were utilized in isolated applications. With the advent of networking and Internet technologies these systems are now being interconnected and remotely addressed. Utilizing these new networking technologies has resulted in significant productivity gains, but at the expense of making these systems vulnerable to cyber intrusions. Developing a business case to protect these systems is difficult as there has been extreme reticence to publicly identify control system cyber security intrusions, whether they are intentional or unintentional. Control system cyber security incidents have occurred in all industries throughout the world. The impacts range from trivial, to significant equipment and environmental damage. This paper provides a technical background of what makes control systems different than IT systems, examples of control system impacts, recommendations for what can be done today to better secure these systems and issues that can affect legal and law enforcement proceedings.

1.0 What Makes Control Systems Different

Control systems comprise SCADA systems, Plant DCSs, PLCs, Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), intelligent field devices and drives, smart meters, etc. SCADA, DCS, and PLCs consist of operator interfaces that are generally Windows, UNIX, or LINUX-based and field devices utilizing proprietary Real Time Operating Systems (RTOSs). Industrial control systems utilize operator interfaces that are similar to traditional IT business systems but the controllers and field devices are fundamentally different than traditional IT systems. For traditional business systems, the paradigm of CIA – Confidentiality, Integrity, and Availability defines the technologies needed to secure the systems. As confidentiality is most important, cryptography is critical. For control systems, the paradigm is the opposite and availability and message integrity are most important. This leads to potentially different technological and policy solutions. Control systems were designed for functionality and reliability/availability rather than cyber security. Specifically, control systems have design characteristics that differentiate them from traditional IT environments.

Table 1
Typical Differences Between Office IT and Control Systems

Attribute	Office IT	Control Systems
System Life Cycle	3-5 years	15-25 years
Confidentiality	High	Low
Message Integrity	Low-moderate	Very High
Availability	Low-Moderate	Very High
Time Criticality	Delays tolerated	Critical
Security skills/awareness	Good	Usually poor
Patching	Frequent	Slow or impossible
Software changes	Frequent, formal, and documented	Rare, informal, not always coordinated
Automated tools	Widely used	Limited, used with care
Communication protocols	IP	DNP, ICCP, Modbus
Communications	Telco, wi-fi	Telco, radio, satellite, power line carrier, wi-fi
Computing resources	High	Very limited
Bandwidth	High	Limited
Security standards	ISO-17799	ISA SP99, etc
Administration	Centralized	Localized
Operating systems	COTS (Windows)	COTS for HMI, proprietary real time for field devices
Security impacts	Business	Business, equipment, personnel safety, and environment
Forensics	Often available	Almost non-existant

- *Deterministic response*: The users expect response to their inputs in a second or less. Application response (e.g., interaction with a remote device) is often measured in milliseconds. The entire environment must act in concert to reliably and consistently provide the deterministic level of response under all system conditions.
- *Ultra-high Availability*: The systems must be operational 24 X 365. Users are reliant on these systems continuously, and even small periods of downtime mean that the associated critical system is unobservable. In the case of an energy utility, response to primary system events is therefore impaired, with associated liabilities.
- *Proprietary Environments*: Meeting the response and availability requirements often requires the use of special purpose hardware, software (including operating systems), and communications. The intelligent devices and communications networks are typically resource constrained, and may rely heavily on fixed prioritisation and predictable system resource response.

Most control systems in use today were designed to perform specific tasks and contain only limited processing power and memory. Therefore, they don't have the computing resources needed to leverage the authorization, authentication, encryp-

tion, intrusion detection and filtering capabilities of modern security technology. These constraints preclude the use of technologies like block encryption and Public Key Infrastructure (PKI) without seriously degrading control system performance. These technologies are too resource-intensive for many legacy control systems and may actually cause the systems to fail as they attempt to keep up with the intensive demands on their limited resources. In addition, although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Because of this, vendor-provided software patches may be either incompatible with the customized version of the operating system or difficult to implement without compromising service.

The fundamental technical problem with securing control systems is the impact on performance. The fundamental culture problem is that Operations and Maintenance (O&M) personnel are measured by system reliability and availability, not security. Security policies, testing, and technologies exist, or can be readily modified, to protect the operator interfaces. However, traditional IT security policies, testing, and technologies can significantly impact the operation of real time controllers and field devices. Therefore, there is a need to develop security policies, testing, and technologies to protect the real time controllers and field devices. Often times, systems must be "opened up" to vendors and others to optimize performance or minimize potential down time even though this creates cyber vulnerabilities. It should also be noted that there is still a significant "us vs. them" attitude between the control system community and IT. This needs to be overcome as the technologies for control systems and IT systems are blurring. In fact, the control systems community often uses IT infrastructure (*e.g.*, LANS, WANS, firewalls, IDS, VPNs, etc.) for control system networks.

2.0 Control System Cyber Security Expertise

The area of control system cyber security is relatively new compared to traditional IT security. There is a dearth of people who truly understand control system cyber security, possible less than 100 worldwide (see Figure 1). As can be seen from Figure 1, most of the people entering the area of "SCADA Security" are not control system engineers. Rather, they are information security experts without the same grounding in the field of control system design, operations, and maintenance as control system engineers. This can lead to unintentional reduction in control system availability if inappropriate policies are applied or testing performed. Table 1 provides a listing of popular control system cyber security myths. There are few resources available for training or education that deals specifically control system cyber security. At a recent U.S. Department of Homeland Security (DHS)-National Science Foundation (NSF) workshop, it was evident that the universities need specific course material. Additionally, security certifications such as the CISSP and CISM have no test questions that directly relate to control system cyber security.

Table 2
Common Control System Cyber Security Myths

Myth	Reality
IT security policies are adequate	IT policies many not be adequate or appropriate for control systems
Firewalls make you secure	Firewalls are only as good as the riles employed
VPNS make you secure	VPNs provide a secure tunnel for the data entering – VPNs do not ensure the data is trusted – generally, people do not question the validity of information coming from a VPN
Encryption makes you secure	Encryption scrambles the information- it does not ensure the data is trusted- generally, people do not question the validity of information that has been encrypted
IDSs can identify potential control system attacks	IDs have not been trained to recognize control system specific attacks
TCP/IP messaging can be one-way	TCP/IP message requires two-way acknowledgement for session initiation
Field devices can't be hacked	Field devices have been hacked
You can keep hackers out	It is very difficult to keep a knowledgeable, dedicated hacker out
You are secure if hackers can't get in	Intentional or unintentional internal threats also exist
More and better technology can solve security problems	Without appropriate security policies and procedures, any technology can be circumvented

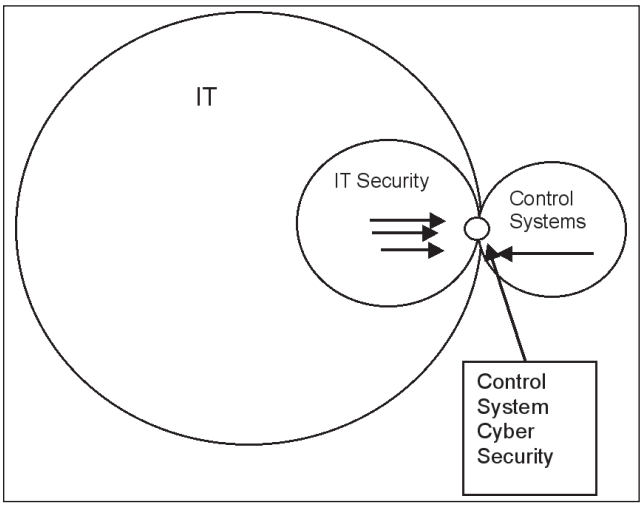

Figure 1 *Control System vs IT Security Expertise Why Are There So Few Experts*

3.0 Control System Vulnerabilities

Control systems offer some of the most attractive targets since they contain the enterprise's most critical data. If an intruder is able to access one of these systems, they would have access to operational data critical to the operation of the system. Additionally, it could also enable a knowledgeable attacker to modify the data used for operational decisions, the programs that control critical industry equipment or the data reported to control centers, the resulting impact could be extremely destructive. Such attacks can cause equipment design and safety limits to be exceeded, potentially causing damage, premature system shutdown, disablement of control equipment and interference with safety system operation. The consequences include endangerment of public health and safety, environmental damage, and/or significant financial impacts due to loss of power production, generation or distribution. Several other critical factors have also contributed to the escalation of risks specific to control systems, most notably the adoption of standardized technologies with known vulnerabilities, connecting control systems with other networks, insecure remote connections and the widespread availability of technical information about control systems. Table 2 provides a listing of typical control system threats and exploits that have been found in actual practice.

When access is available, weaknesses can be exploited. Utilizing those weaknesses, control system researchers at the U.S. Department of Energy's national laboratories have publicly demonstrated the feasibility of cyber attacks on control systems at electric power facilities and chemical facilities. Using tools readily available, they have modified input from Corporate Networks, Control Networks, and field devices. Figure 2 is a typical network configuration utilized in one of the demonstrations. The compromised packets needed to pass through two sets of firewalls before reaching their ultimate target, the SCADA LAN. Once reaching the SCADA LAN, the compromised packets were able to take over direct control of control center SCADA and substation LANs as well as modifying operator screens. The demonstrations have also been able to change settings and create new output that could incapacitate substations and open valves in power plants and other process facilities.

Table 3
Typical Cyber Security Threats and Exploits

Threat	Exploit
Disgruntled employee	New/modified files
Viruses/Worms/Trojans	New sockets/new processes
Prohibited software	Removable media/games
Vendor updates	Files modified
Software malfunction	Process termination
Hacker reconnaissance	NIDS alert
Contractors	Rogue devices
Inappropriate policies/testing	Control system performance degradation

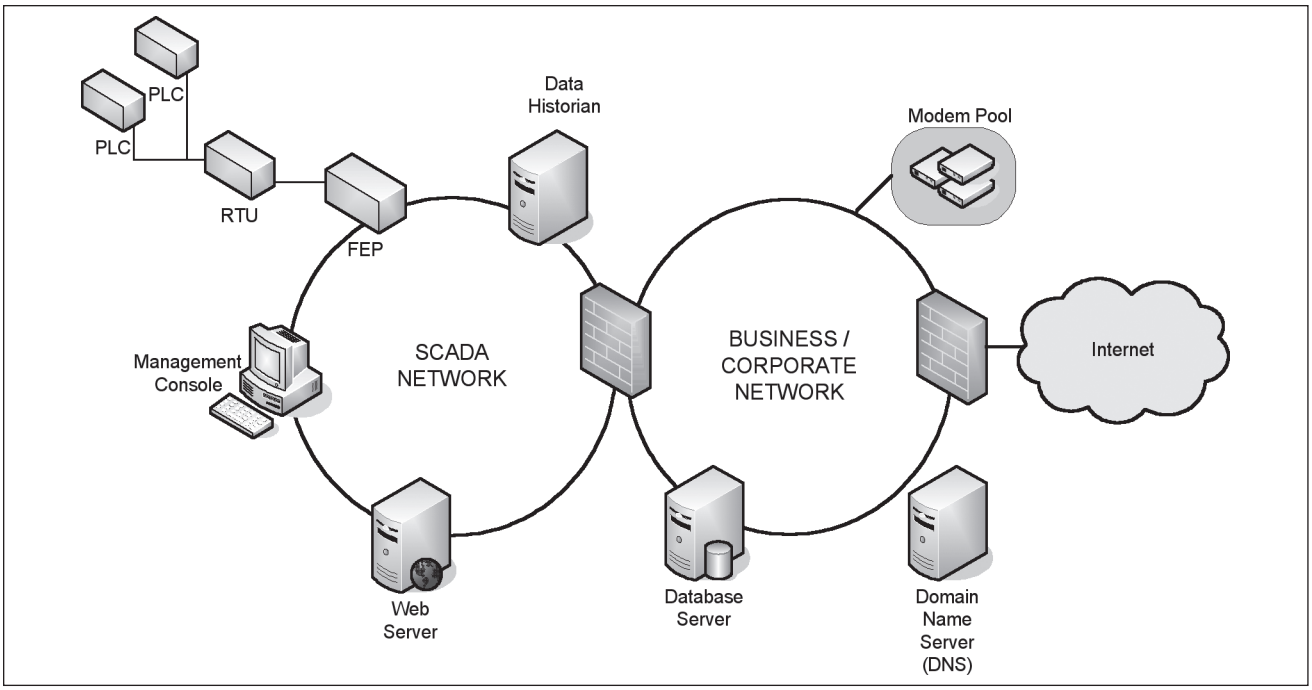

Figure 2 *Control System Cyber Security Vulnerability Demonstration*

Many forms of remote access have caused control center vulnerabilities. Insecure communication protocols between control systems and insecure applications of tools, such as ActiveX controls, cause further risks. Damage can range from loss of confidential data to altering data resulting in erroneous equipment operation or operator information leading to miss-operation. Many operational facilities have no firewalls or electronic intrusion detection systems. Often, the only indication of an attack will be the damage caused by the intrusion. Control systems and transient monitoring systems have been designed to identify and trend potential physical system impacts not electronic intrusions.

As mentioned previously, control systems generally utilize two operating systems. One is at the operator station that has the capability for role-based access, encryption, and other information security technologies. The other is at the "distributed processing unit," where the sensor information is collected and calculations made. These are RTOS that are usually proprietary systems. The RTOS have been configured with specific prioritization and communication threads. Information security policies have not been included in the kernel of these systems. Consequently, these RTOS do not have the capability to make the requisite calls to authorize, authenticate, or encrypt/decrypt before data is sent. Additionally, RTOS dedicate most of their resources to performing calculations related to system operational performance. Security is viewed as an overhead function.

4.0 Field Results

Based on the numerous vulnerability assessments performed by KEMA in North America, South America, Europe, and Asia there have been several common findings:

- *Dial-up modems*: Almost all utilities had modems they were unaware of and modems that were not supposed to be connected that were connected;
- *Security policies*: Almost all existing security policies were IT policies and did not address control system-unique issues;

- *Configuration control*: Almost all utilities had ”rogue” programs and/or applications on critical systems;
- *Architecture*: Many utilities had their control networks directly connected to the Corporate LAN, though often in an inconspicuous manner; and
- *System integration*: Many utilities did not address the vulnerabilities of other systems that were being integrated into SCADA or the plant DCS.

5.0 Need for a Quantitative Business Case

All industries including electric power are in need of a quantitative business case that documents the impacts of cyber incidents. Currently, it is difficult, if not impossible, for operational managers to perform economic trade-offs between O&M expenditures and control system cyber security mitigation. Consequently, a study is being performed to develop representative case histories of companies that have had their control systems impacted by cyber (some of these are transmission and distribution cases). Results to date are:

- Companies are very reticent to report control system cyber security incidents;
- Control system cyber security impacts can be very expensive even if power is not interrupted;
- Penetration testing and scanning of control systems is causing a growing number of control system impacts; and
- Most of the cases identified to date could have been prevented or mitigated with adequate control system cyber security procedures.

6.0 Control System Cyber Impacts

There are three major categories of cyber impacts:

- Unintentional impacts caused by inadequate or inappropriate security policies or testing;
- Unintended impacts caused by viruses or worms that were created to attack general purpose operating systems, etc. that have been integrated with control systems; and
- Intentional targeted attacks.

Generally, the first category is the most probable, but generally has short-term impacts. The second category is also probable, but generally causes denial of service of communications or operator awareness. While a problem, it generally is not directly life-threatening or a threat to control system integrity. The third category is by far the most significant, but also the lowest probability as it generally requires detailed knowledge of the systems and their vulnerabilities.

There have been more than 80 cases where control systems have been impacted by cyber in electric power, water, oil/gas, chemicals, and manufacturing. These cases have occurred in North America, South America, Europe, and Asia. Impacts have ranged from trivial to significant equipment and/or environmental damage to deaths. The majority of the control system cyber cases to date have been unintentional or virus/worms. In most cases, appropriate control system security policies and procedures could have either prevented the event or minimized the impacts.

7.0 What Can Be Done Now

Prudence dictates that a control system cyber security program be developed for these critical systems. The following aspects can form a prudent control system cyber security program:

1. Governance:
   - Get active senior management support.
   - Identify who is responsible and who needs to be involved.
   - Make the organization known to all throughout the enterprise.
   - Make sure the program is reviewed periodically.

2. Awareness and Training:
   - Make the training and awareness appropriate.
   - Specifically address control systems as IT awareness and training may not be appropriate for control systems. Include traditional IT security awareness and training for non-control system applications.
   - People tend to want to do what is best so tell them what is expected of them and why.

Policies and Procedures:
- Make them appropriate and prudent by specifically address control systems. Control system cyber security policies and procedures are different than IT. Ensure that the control system policies and IT policies are consistent.
- If they aren't written down, they probably aren't being followed - modem access is a classic example.
- Map the policies to industry or regulatory standards and guidelines where appropriate.
- NERC CIPC 002-009, ISO 17799, ISA SP99, AGA12, prudent engineering practices, etc.
- ISO 17799

3. Perform Vulnerability/Risk Assessments:
   - Identify all known vulnerabilities in a device or architecture. It is important to know what is installed. Scans can impact control systems and do not always identify all open ports or identify modems.
   - Perform risk assessments try to prioritize vulnerabilities and assess the impact. Good probabilities for risk assessments are not available, but vulnerabilities can be prioritized. Risk assessments are a good way to involve the stakeholders in the process and get acceptance.
4. Configuration Management:
   - Document the field configuration and status of hardware and software, including security patches. Maintain a list of individuals who should be notified of pending changes. Enforce a time limit in which changes are reviewed before being implemented. Require back out procedures in case something goes wrong. Require and maintain documentation of what tests were performed on the proposed change.
5. Secure Architecture:
   - Identify your critical assets.
   - Define the electronic perimeter for your control environment.
   - Isolate the control environment using firewalls to the extent possible with no access by default.
   - No connections initiated from the outside to the extent possible. Try to pull data into or push data out of the control environment. Don't allow devices on the outside to push data in or pull data out.
   - Allow only needed services and ports which is not always possible to do for control systems and devices.
   - Don't allow browsing of the Internet or incoming e-mail from the control environment.
   - Keep unauthorized devices out.
6. Remote Access:
   - Should be severely restricted.
   - Don't allow devices on the outside to become part of the Control Network.
   - Use VPNs where appropriate.
   - Do not allow split tunneling.
   - Require anti-virus and personal firewalls, where it doesn't affect performance.
   - Enforce patch levels on software, where possible.
   - Try to avoid dial-up modems which are not always possible even with new control system equipment. Where possible,

use dial-back modems, encrypting modems, or other security approaches are advised.
    - Think of wireless (802. – Wi-Fi) as remote access and use encryption, directional antennas, etc. Be careful in using wireless for any critical control loops.
7. Patch management:
    - Patch management deals with testing and applying patches released for installed products.
    - Control systems may not be able to utilize non-customized patches. Avoid automated patch management tools for control systems. Assure that control system vendor will support the patch. Test on your system before applying in an operating environment!
8. Monitoring:
    - Anti-Virus is needed for the Windows environment, but be careful. Anti-virus can impact control system performance.
    - Host Intrusion Detection Systems (IDS)/Intrusion Prevention System (IPS) generally require about 5% of system resources. Control systems may not have available resources. Identify what really needs to be monitored. Existing IDS/IPS may not be appropriate for control system networks and could cause control system performance impacts – TEST!
    - Network IDS/IPS are "passive" in that they do not cause latency in network traffic.
    - IPS's rely on detecting anomalies which is difficult to train in chaotic Corporate environment. The more stable Control System environment might be ideal for anomaly-based intrusion detection systems if appropriately designed.
9. Incident Response:
    - Needs to be tailored to identify who is in charge, where to get emergency approvals. Need to recognize that cyber is different and team membership can be different in different circumstances.
    - Table top drills need to be formalized with clear communication. Need to expect and plan to be ignored or not be sufficient. However, recall the adage that "Planning is essential, but plans are worthless."

8.0 Legal and Law Enforcement Issues

There are several issues with control systems that can impact law enforcement and legal proceedings following a control system cyber event.

1. **Forensics:** With the exception of modern control center SCADA systems, there often are no logs that collect communications between control system devices. In other cases, the logs are erased when power is removed. Additionally, many field facilities do not have firewall logs or intrusion detection logs. There often are shared logins that make it difficult to which specific individuals have logged in. Availability of control systems are critical for continued operation of critical processes. For general IT, the affected computer can be quarantined following a cyber event until all data and files have been thoroughly examined. With control systems, the control system needs to be returned to service in the most expeditious manner possible. The systems cannot be "yellow-tagged" while the investigation continues. Because control system cyber security can be affected by the cyber communication between systems, event diagnostics can be problematic unless there is a complete mirror image of the software, hardware, and integrated systems.

2. **International issues:** Approximately half of the industrial control system suppliers

are based in North America. Additionally, many large control system users are multinational and communicate globally. Consequently, there is a need to assure that international agreements are in place to complete investigations.

3. **Information Sharing:** There has been an extreme reticence by private industry to share control system cyber impact information with the government. Consequently, the majority of control system cyber events to-date have not been reported to law enforcement or the Information Sharing and Analysis Centers (ISACs). There is also a prevailing feeling that when the government is made aware of threats or events, it is not passed onto the appropriate industry organizations in a timely manner.

Recommendations

1. Develop forensics for control system cyber security.
2. Include the control system community in the investigations.
3. Establish a CERT for Control Systems with control system expertise and industry credibility. Use this interface to "sanitize" information prior to reaching the government so as to minimize disclosure issues. Provide timely, useful feedback.

Summary

Cyber vulnerabilities are real. They can, and have impacted control system operation. It is crucial that the end-users understand the impacts of control system cyber security and have plans to address trying to prevent an intrusion, but also how to deal with an intrusion when it occurs. A good control system cyber security program provides due diligence and can potentially maintain or improve control system reliability and availability. Coordinating legal and law enforcement issues with the control system community can help both the legal and operational communities address their respective concerns.

Chapter 5

Political Structure

Synopsis

5.1 *Creating an Information Sharing Environment in a Post-9/11 World* by Richard Weitz

5.2 *Preventing the Poisoning of the Well: A Consideration of the Necessity and Legality of Broadening the Protection of Critical Infrastructure Information in the Interest of National Security and Public Safety* by Paul D. Barkhurst

5.3 *Federal Preemption of State Open Records Laws After September 11* by Stephen Gidiere

5.4 *Federal Freedom of Information Act-Driven Coverage of the Department of Homeland Security: A Pilot Study* by Charles Davis

5.1 Creating an Information Sharing Environment in a Post-9/11 World

by Richard Weitz

The terrorist attacks of September 11, 2001, exposed major gaps in how the U.S. political structures had transitioned from the old threats of the Cold War to the new challenges of the post-9/11 world. In response, political authorities at the federal, state, and local levels—as well as influential policy makers within the business and nonprofit sectors—have struggled determine how Americans can strike the optimal balance between the public's right to access public information and the requirement to protect genuine secrets from assisting hostile terrorist groups.

The U.S. National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) identified information sharing as a glaring weakness in the United States' ability to combat terrorism and ensure homeland security. Recognizing that lingering Cold War procedures have prevented executive departments and agencies from effectively managing current threats to U.S. national security, the 9/11 Commission recommended that the United States establish policies for sharing terrorism information more effectively across federal, state, and private sector entities.[1]

In the period leading up to the 9/11 attacks, the CIA and FBI had each gathered information on several of the hijackers. Nevertheless, legal restrictions and a cultural predisposition in favor of safeguarding rather than sharing information prevented the timely integration and evaluation of this data.[2] For example, the reluctance of the FBI and the CIA to exchange information with other agencies meant that in September 2001, the Federal Aviation Administration's no-fly list catalogued the names of only twelve potential terrorists. None of these individuals matched the identities of the al-Qa'eda hijackers who would attack the United States that morning.[3]

Since the report's publication, the United States has made considerable progress towards establishing an Information Sharing Environment (ISE) in which public and private actors at all levels can manage information securely but also sufficiently effectively to allow for the timely assessment of

1 National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 2004, *available at* http://www.9-11commission.gov/report/911Report.pdf [hereinafter National Commission on Terrorist Attacks].

2 *Ibid.*

3 Government Accountability Office, *Progress Has Been Made to Address the Vulnerabilities Exposed by 911, But Continued Federal Action is Needed to Further Mitigate Security Risks*, Jan. 24, 2007, http://www.gao.gov/new.items/d07375.pdf.

threats and vulnerabilities. Yet, much work remains given the substantial evidence that a terrorist threat to the U.S. homeland persists.

The need to reform terrorism information sharing policies remains urgent. In an August 2007 report, the New York City Police Department's Intelligence Division identified at least ten major instances since 9/11 in which state and local law enforcement agencies, the FBI, and European police and intelligence agencies cooperated to disrupt terrorist plots by "homegrown actors" who had little of any support from al-Qa'eda or other foreign terrorist movements. The authors warned that the number of homegrown Islamic radicals appeared to be growing, establishing a basis for future terrorist threats.[4] These homegrown Islamists communicate with other radicals through jihadist websites and local "radicalization incubators" such as mosques, cafes, prisons, student associations, and hookah bars.[5] Local law enforcement officials, who are often in the optimal position to observe homegrown terrorist threats, must be able to effectively provide information on the threat posed by domestic radicals to federal partners with counter-terrorism functions.

The threat of international terrorism also remains disturbingly great. Then Attorney General Alberto Gonzales reminded his audience at the recent Global Initiative to Combat Nuclear Terrorism Law Enforcement Summit of Osama bin Laden's persistence in trying to obtain nuclear weapons over the course of more than a decade.[6] Gonzales called combating nuclear terrorism the "challenge of our generation as law-enforcement and intelligence professionals" and claimed that "communication, sharing, and coordination" must be "applied in combating the proliferation of WMD and their many components."[7]

Yet, civil liberty groups, privacy advocates, and other concerned individuals have expressed alarm that the sharing of data within the United States and with foreign countries would unduly compromise Americans' fundamental rights for questionable progress in the war on terrorism. After the United States and the European Union agreed in June 2007 to renew their agreement to share personal data about millions of U.S.-bound transatlantic airline passengers, Stavros Lambrinidis, a member of the European parliament from Greece and vice chairman of that body's civil liberties, justice and home affairs committee, warned that the new accord represented dangerous "function creep" by allowing the information to be used for non-terrorist crimes.[8]

Many privacy advocates also expressed alarm after the Director of National Intelligence, Michael McConnell, agreed in August 2007 to work with the Department of Homeland Security to allow more federal and local authorities to access data from U.S. reconnaissance satellites for counterterrorism and other law enforcement purposes. Steven Aftergood, director of the Project on Government Secrecy for the Federation of American

4 Mitchell D. Silber & Arvin Bjatt, *Radicalization in the West: The Homegrown Threat* (New York City Police Department) 2007, *available at* http://www.nyc.gov/html/nypd/pdf/dcpi/NYPD_Report-Radicalization_in_the_West.pdf.

5 *Study: Local Law Enforcement in Best Position to Monitor Potential Terrorists*, Associated Press, Aug. 15, 2007, *available at* http://www.wreg.com/Global/story.asp?S=6937014; Dan Eggen, *Terror Threat Grows Quietly, Report Warns*, Wash. Post, Aug. 16, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/08/15/AR2007081502156_pf.html; Richard Weitz, *Countering Islamic Terrorism in U.S. Prisons,* Psi.praeger.com, Mar. 15, 2007, available at http://psi.praeger.com/doc.aspx?d=/commentary/Weitz1.xml.

6 Attorney General Alberto R. Gonzales, "Remarks at the Global Initiative to Combat Nuclear Terrorism Law Enforcement Summit," June 11, 2007 (transcript available at http://www.usdoj.gov/ag/speeches/2007/ag_speech_070611.html).

7 *Ibid*. Additional information on this conference is available in Richard Weitz, *The Global Initiative to Combat Nuclear Terrorism Drives Forward*, WMD Insights, no. 17, pp. 17-23, July-Aug. 2007.

8 Paul Lewis & Spencer S. Hsu, *Travelers Face Greater Use of Personal Data*, Wash. Post, July 27, 2007, at 7.

Scientists, acknowledged that the program could be useful but quickly added that it "comes with risk to privacy and to the integrity of our political institutions."[9] Kate Martin, director of the Center for National Security Studies, warned that the move toward "Big Brother in the sky" is "laying the bricks one at a time for a police state."[10]

Some specialists complained that, since the U.S. Department of Defense owns many of the satellite systems, their use for law enforcement purposes would violate the Posse Comitatus Act.[11] The courts have never ruled on the permissibility of warrantless searches of private property by spy satellites. A 2005 study commissioned by the U.S. intelligence community cautioned that "There is little if any policy, guidance or procedures regarding the collection, exploitation and dissemination of domestic MASINT" ["Measurement and Signatures Intelligence"].[12]

This paper provides a context for assessing research into state anti-terrorism legislation and open government laws and practice by examining primarily federal changes designed to create an ISE. The first section reviews these changes and describes the policies and procedures underpinning the ISE. It devotes much attention to the national implementation strategy, legal framework, and civil liberties issues affecting the ISE process. The second section of the paper examines the information sharing initiatives that have been launched by the defense, homeland security, intelligence, and law enforcement communities, as well as the private sector. This section evaluates both the progress that has been achieved since 9/11 as well as remaining technical, cultural, and strategic challenges to creating a genuine information sharing environment. The paper ends with some preliminary conclusions and recommendations for improving ISE implementation.

I. An Approach to Information Sharing

The Information Sharing Environment (ISE) consists of policies, procedures, and technology that permit the exchange of terrorism information, including intelligence, homeland security, and law enforcement data. The ISE, which is "not a place or an information system" but rather a policymaking "approach," connects federal, as well as state, local, and tribal (SLT) governments.[13] The ISE also envisions a critical role for private sector and foreign actors in sharing information to counter terrorist threats. Created by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[14] the ISE is intended to advance a culture of sharing among its participants and ensure that information is readily available to support its participants' missions.

In May 2006, Ambassador Ted McNamara, the current program manager for the Information Sharing Environment (PM-ISE), explained to Congress the four-fold mission of the ISE. The foremost aim of the ISE is to establish a "trusted partnership"[15] among ISE participants, a collaborative relationship that promotes vigorous information exchange. Recognizing that a flow of terrorism information is only beneficial when it is exchanged with appropriate actors, verified for accuracy, and managed in accordance with legal protections on privacy and security, McNamara stated that the second chief objective of the ISE is to establish policies that effectively coordinate terrorism information sharing. McNamara insist-

9 Cited Joby Warrick, *Domestic Use of Spy Satellites To Widen*, Wash. Post, Aug. 16, 2007, at 1.

10 *Ibid*.

11 Eric Schmitt, *Liberties Advocates Fear Abuse of Satellite Images*, N.Y. Times, Aug. 17, 2007.

12 Cited in Robert Block, *U.S. to Expand Domestic Use of Spy Satellites*, Wall St. J., Aug. 15, 2007, at 1.

13 Ise.gov, Program Manager, Information Sharing Environment, http://ise.gov/ (last visited Jan. 19, 2008) [hereinafter Ise.gov].

14 Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485 (2004).

15 *Challenges of Information Sharing Implementation*, CQ Congressional Testimony, May 10, 2006 [hereinafter *Challenges of Information Sharing Implementation*].

ed that, "We want to get the right information, to the right people, at the right time to ensure success."[16] Third, in order to enhance the content and usefulness of shared information, the ISE is designed to be a "decentralized" and "distributed" system that addresses the needs of multiple public and private sector partners but also harmonizes sharing through common practices and quality standards.[17] Finally, the ISE seeks, to the greatest extent possible, to build upon existing capabilities for information sharing and to develop innovative strategies and technologies to augment current efforts.[18]

In the long term, the ISE is intended to create marked cultural change in government operations by eroding "need to know" policies on the handling of intelligence and national security information. The "need to know" approach, which stems from Cold War procedures, holds that individuals and entities requiring information can be identified before any sharing takes place. Access regulations, formulated in advance, can thus provide information to those who "need to know" and exclude all others.[19] The "need to know" approach creates an environment hostile toward sharing by encouraging officials to guard information to a maximum degree. However, this hostility is poorly suited for managing terrorism information, which is often collected by diverse members of the intelligence, homeland security, and law enforcement communities but must be synthesized in order to provide a coherent picture of national security threats.

"Need to know" policies must therefore give way to the development of a "need to share" culture. Under a "need-to-share" regime, ISE participants will understand that the benefits of sharing information in a post-9/11 world far outweigh the risks. Through training, collaboration, and coordinated information exchange efforts, they will develop the trust necessary to overcome the "need to know" mentality. Though one of the ISE's most significant long-term goals, effecting cultural change, is likely to be challenging. In a statement to Congress in 2005, Lee H. Hamilton, former Vice Chair of the 9/11 Commission, emphasized that altering ISE participants' mindsets will require persistent effort. "You can change the law, you can change the technology, but you still need to change the culture; you still need to motivate institutions and individuals to share information,"[20] he reminded Congress.

Over time, however, a well-managed ISE will deconstruct perceptions that individuals and institutions misinterpret or misuse information that is initially collected by others. Director of National Intelligence Mike McConnell has stated that as "need to share" policies overcome hostilities toward information sharing, the ISE itself should evolve to embrace a "responsibility to provide" strategy.[21] By fostering a culture in which information sharing is not only encouraged but also obligatory, ISE participants can achieve a "high[er] degree of coordination and interaction to improve our collective intelligence capability."[22]

Role of the Program Manager

The office of the program manager was created by section 1016(f) of the IRTPA to oversee implementation of the ISE. Though the program manager was initially slated to serve a two-year tenure,[23] his position has been extended until the year 2009 to enable him to supervise completion of all phases of the ISE Implementation Plan.[24] The

16 *Ibid.*
17 *Ibid.*
18 Ise.gov, *supra* note 13.
19 National Commission on Terrorist Attacks, *supra*, note 1.
20 *Role of the Information Sharing Program Manager in Homeland Security*, CQ Congressional Testimony, Nov. 8, 2005 [hereinafter *Role of Information Sharing*].
21 *Creation of New Information Sharing Steering Committee for the Intelligence Community*, PR Newswire-US Newswire, Mar. 6, 2007.
22 *Ibid.*
23 6 U.S.C. §485(f)(1) (2004).
24 Program Manager, Information Sharing Environment, *ISE Implementation Plan*, Nov. 2006, http://ise.gov/docs/ise-impplan-200611.pdf [hereinafter *ISE Imple-*

program manager's office is small, consisting of roughly fifteen to twenty-four employees,[25] but is delegated wide authority to create a plan for ISE implementation, develop strategies to promote and coordinate information sharing, and assess the ISE's progress by submitting regular reports to Congress. Current program manager McNamara has stated that his role is best understood as that of a "facilitator."[26]

On May 20, 2005, President Bush appointed John Russack, formerly the director of intelligence at the Department of Energy, as the first program manager. However, Russack found that his office was understaffed and under-funded and he experienced considerable difficulties in beginning the process of launching the ISE.[27] Some confusion surrounding Russack's responsibilities arose early on in his tenure, as the IRTPA had failed to designate the official to whom the program manager reports. In March 2005, the Commission on Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction noted the problem, stating that "The confused lines of authority over information sharing created by the intelligence reform act should be…reconciled and coordinated."[28]

A June 2005 presidential memorandum rectified the omission by placing the program manager within the Office of the Director of National Intelligence (ODNI), then under the direction of John Negroponte.[29] Critics, however, were quick to point out that the decision significantly weakened the intended role of the Department of Homeland Security in creating the ISE.[30] They further contended that the responsibility of overseeing the program manager would likely distract the DNI from his other duties.[31] Others complained that the decision placed undue emphasis on the role of the intelligence community in the ISE, to the detriment of other participants.[32] McNamara has attempted to refute such a perception in stating, "We're [the office of the program manager] not an intelligence agency; that is, we're not just concerned with intelligence. We're responsible for all terrorism information, whether or not it's intelligence. And there is a lot of information out there; in fact most of it, which is not intelligence."[33]

The difficulties of operating under the direction of the DNI have been cited as a reason for Russack's resignation in January 2006.[34] Russack's departure challenged Congress and the President's goal of achieving timely establishment of a functional ISE. As Illinois Senator Dick Durbin commented, Russack's resignation was a "troubling setback" and showed that "our best efforts to implement 21st-century for information-sharing [were] still far behind."[35]

In March 2006, President Bush named Ambassador Ted McNamara, formerly the head of counterterrorism at the State Department, as Russack's successor.[36] McNamara assumed his role with a

mentation Plan].

25 *Challenges of Information Sharing Implementation*, *supra* note 15.

26 Ted McNamara, Program Manager, Information Sharing Environment, *Remarks at the DNI's Information Sharing Conference and Technology Exposition*, Federal News Service, Aug. 22, 2006 [hereinafter McNamara Remarks].

27 Patrick Yoest, *Sharing of Information on Terrorism Intelligence Draws Fire, Presents Challenges*, Apr. 18, 2006 [hereinafter Yoest].

28 Memorandum on Strengthening Information Sharing, Access, and Integration—Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment, Pub. Papers, June 6, 2005, *available at* http://www.fas.org/sgp/news/2005/12/wh121605-memo.html [hereinafter Memorandum on Strengthening Information Sharing].

29 *Ibid*.

30 *Challenges of Information Sharing Implementation*, *supra* note 15.

31 *Ibid*.

32 *Ibid*.

33 McNamara Remarks, *supra* note 26.

34 *Challenges of Information Sharing Implementation*, *supra* note 15.

35 Shaun Waterman, *Replacement of Infoshare Boss Spells Delay*, UPI, Feb. 7, 2006.

36 *Challenges of Information Sharing Implementation*, *supra* note 15.

fresh and energetic attitude.[37] Despite delay caused by Russack's resignation, McNamara's office released its ISE Implementation Plan in November 2006. McNamara remains aware, however, of the challenges he faces in achieving "progress" in implementing the ISE, promoting "technological consistency," and ensuring "policy compliance" among the ISE's participants.[38]

McNamara emphasizes that the office of the program manager plays an essential role in ISE implementation but is "not a substitute"[39] for effective leadership within the ISE's participating federal departments and agencies. McNamara's management and oversight function also requires a strategic partnership with and the continued support of Congress.

Lee H. Hamilton, former Vice Chair of the 9/11 Commission, told Congress in a 2005 hearing that the program manager's success is largely dependant on Congress' willingness to provide his office with sufficient resources.[40] Because section 1016 of the IRTPA does not address the program manager's budget, another gap in the statutory language tending to suggest that the creation of the ISE was advanced without careful consideration of its complexities, it is essential that Congressional oversight of ISE implementation supplement the program manager's efforts. As the program manager's role is central to the deployment of the ISE, Hamilton has urged that the program manager also receive "strong support from the President and the direct engagement of senior leadership of the Homeland Security Council"[41] in carrying out his mandate.

The Information Sharing Council

The Information Sharing Council (ISC), established by section 1016(g) of the IRTPA, is an advisory body that assists the President and the program manager, its chair, in "developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE."[42] The ISC had its first meeting in November 2005, and has since continued to meet on a regular basis.[43]

Membership of the ISC consists of the Department of Commerce, Central Intelligence Agency, Department of Defense, Director of National Intelligence, Department of Energy, Federal Bureau of Investigation, Department of Health and Human Services, Joint Staff, Department of Homeland Security, National Counter Terrorism Center, Department of the Interior, Office of Management and Budget, Department of Justice, Department of State, Department of Transportation, and Department of Treasury.[44] The body has two standing subcommittees, the State, Local, and Tribal Subcommittee and the Private Sector Subcommittee, as well as several ISC Working Groups that assist members in performing their advisory functions.[45]

Despite the role of the State, Local, and Tribal Subcommittee, the ISC has been criticized for its exclusively federal membership and the general lack of SLT representation.[46] McNamara has stated that it is his "intention as chair of the ISC to keep in close contact with state, local, tribal, and private sector partners through regular meetings with them and by inviting them to work closely with the ISC."[47] However, critics posit that such an intention can only be fulfilled if those partners

37 *Ibid*.
38 *Ibid*.
39 McNamara Remarks, *supra* note 26.
40 *Role of Information Sharing*, *supra* note 20
41 *Ibid*.
42 6 U.S.C. § 485(g)(2)(A) (2004).
43 *The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, Government Accountability Office, Mar. 17, 2006, available at http://www.gao.gov/new.items/d06385.pdf. [hereinafter *Federal Government Needs to Establish*]
44 Ise.gov, *supra* note 13
45 *Ibid*.
46 *Challenges of Information Sharing Implementation*, *supra* note 15.
47 *Ibid*.

are full members and in a position to influence recommendations made directly to the President and program manager.

Consistent with the requirements of the IRTPA, however, the ISC has provided the President and PM-ISE with recommendations addressing specific challenges to ISE implementation, including technological questions and the problems caused by the over-classification and pseudo-classification of terrorism information.[48] The ISC has also guided the allocation of ISE resources and assists PM-ISE McNamara in deciding how to leverage members' existing sharing capabilities in establishing the ISE.

Implementing the ISE

In mid-November 2006, DNI John Negroponte delivered to Congress the *Information Sharing Environment Implementation Plan* (Plan), a report PM-ISE McNamara called a "roadmap for the successful implementation of the ISE" which "responds to the recommendations of the 9/11 Commission…[and] builds on the progress of the past five years to further improve the way in which we share information and fight terrorism."[49] Developed over the course of a year, the Plan is the product of McNamara and the ISC's close collaboration with officials of fifteen federal departments and agencies, including the Departments of Justice, Homeland Security, Defense, and State, as well as the FBI, and ODNI.[50] The Plan provides overarching strategies to ensure the full integration and active participation of federal, SLT, foreign, and private sector entities. The Plan explains that "[o]nce implemented," its strategies should "facilitate the sharing of analytic products and other information by all information-sharing environment participants."[51]

The Plan sets forth two phases of action items, the first designed to capitalize on and improve sharing capabilities existing at the time of the Plan's issuance and the second calculated to provide a framework for "comprehensive implementation" of the ISE by 2009.[52] While meeting the Phase 2 timetable is crucial for success of the ISE, its action items tend to require more preparation and funding than those of Phase 1, which detail concrete means to meet the most urgent information sharing needs.[53] However, both phases are necessary for the implementation process to culminate in the development of an enduring culture of information sharing that ensures long-term operation of the ISE.

The Plan recognizes that developing a fully functional ISE will require strong oversight and organized management. The Plan therefore recommends that the PM-ISE, whose position was created as a temporary, two-year tenure under section 1016(f)(1) of the IRTPA, remain in office until the completion of Phase 2 of the Plan in 2009.[54] This recommendation has been met with praise, as many ISE participants recognize that the "program manager's position is integral to continued success of the program."[55] Mary Fetchet, Founding Director of Voices of September 11th, and others have told Congress that the PM-ISE should be established as a permanent office.[56] Fetchet commented that a permanent PM-ISE could ensure long-term success of the ISE with "authority to issue government wide standards for information sharing…create incentives for improving information sharing as well as impose sanctions for agencies that fail to share information properly."[57]

48 Siobhan Gorman, *New Chief Faces Pressure to Advance Data-Sharing*, The Baltimore Sun, Mar. 3, 2006.
49 *Information Sharing Environment Implementation Plan Report Sent to Congress*, U.S. Newswire, Nov. 16, 2006 [hereinafter *Information Sharing Environment Implementation Plan Report Sent to Congress*].
50 *Ibid*.
51 *ISE Implementation Plan, supra* note 24.
52 *Ibid*.
53 *Ibid*.
54 *Ibid*.
55 *Implementing Recommendations of the 9/11 Commission*, CQ Congressional Testimony, Jan. 9, 2007 [hereinafter *Implementing Recommendations*].
56 *Ibid*.
57 *Ibid*.

The Technical Front

Though the 9/11 Commission emphasized that creating an ISE has more to do with developing policy and promoting a culture of sharing than creating systems or additional technology, the Implementation Plan discusses several technical initiatives necessary to enhance participants' capacity to share information through the ISE. It is important, however, that the Plan adopts a decentralized approach to technological improvement and avoids the establishment of any collective information systems. A decentralized information sharing environment is more flexible, upgradeable, and better able to meet the needs of its users in a world of evolving security threats.

According to the Plan, technical aspects of ISE implementation are intended to "add value to current and future [ISE processes] in three dimensions,"[58] which include the acquisition of information sharing tools, the expansion of information shared in the ISE, and the development of new capabilities. Phase 1 of the ISE Implementation Plan requires the PM-ISE and members of the ISC to identify developing technology and best practices that will enhance their ability to share information in the ISE. Phase 2 will then build upon previous efforts by incorporating emerging technology into the ISE and assessing capabilities vis-à-vis new needs and security threats.

Though the technological needs of the ISE's participants will vary, Phase 2 of the Plan contemplates the integration of certain key technologies into the ISE. For example, the PM-ISE and ISC support current pilot programs aimed at providing wireless access to Sensitive but Unclassified (SBU) information.[59] Additionally, the Plan encourages speedy implementation of the IRTPA's directive to create Electronic Directory Services (EDS).[60] EDS enables users to identify and locate people and organizations with whom they would like to communicate in the ISE. Though certain small-scale EDS technologies are already available,[61] the PM-ISE is interested in building upon existing technology to provide more accessible and comprehensive means for contact information searches in a large ISE. The Plan contemplates the development of EDS that provide Blue Pages, containing contact information of counterterrorism organizations; Yellow Pages, offering information about the roles and specializations of organizations listed in the Blue Pages; Green Pages, listing data sharing resources; and White Pages, cataloging contact information for individuals.[62]

In order to strengthen interagency sharing initiatives, the Plan also emphasizes the importance of integrating cross-community technological services into the ISE. Cross-community technological services would horizontally connect federal ISE participants across the intelligence, defense, law enforcement, and homeland security communities, as well as facilitate vertical information sharing between federal and SLT partners. Some examples of cross-community technological services include mechanisms for sending and receiving alerts and notifications; logging on to terminals, Web interfaces, and mobile devices containing shared terrorism information; conducting higher-powered searches; and developing complex information "access control" processes that take into account users' roles and security clearances, as well as the level at which data is classified.[63]

Identifying technical development as a "major priority in both phases"[64] of ISE implementation, the Plan stresses that emerging technology and best practices incorporated into the ISE reflect both business and technical expertise. The Plan pro-

58 *ISE Implementation Plan, supra* note 24.
59 *Ibid*.
60 6 U.S.C. § 485(b)(2)(G) (2004).
61 Jason Miller, *Directory Services at the Core of Sharing Intelligence Info*, Gov't Computer News, Sept. 19, 2005, *available at* http://www.gcn.com/print/24_28/37038-1.html [hereinafter Miller].
62 *ISE Implementation Plan, supra* note 24
63 *Ibid*.
64 *Ibid*.

vides for long-term technical support for the ISE's operations by encouraging participants to continually assess their capabilities and changing needs.

Multi-Level Government Sharing and Participation of Non-Government Actors

An effective terrorism information sharing environment must ensure the full integration and participation of not only federal actors, but also key SLT, foreign, and private sector entities. The Plan views multi-level government sharing and sharing with non-government actors as an opportunity to pool expertise and develop a sense "shared responsibility" among participating entities for "the timely processing and dissemination" of terrorism information.[65] Attaining this objective requires that common standards, including privacy laws, guide participants' activities and ensure that each "meet a certain baseline level of capability."[66]

On a cultural level, the Plan recognizes that successful multi-government sharing in the ISE requires deconstructing perceptions that federal and SLT sharing processes are competitive, rather than collaborative. The Plan therefore promotes efforts to homogenize the variety of exiting sharing practices concerning terrorism "alert, tip, advisory, situational awareness, and warning systems."[67] To ensure active participation of SLT officials in the ISE, the Plan also requires the PM-ISE and members of the ISC to reach out to a number of key SLT and interagency actors. These include Joint Terrorism Task Forces (JTTFs), Field Intelligence Groups (FIGs), Information Sharing Analysis Centers (ISACs), and state and local intelligence information fusion centers. The roles, responsibilities, and contributions to the ISE of each of these institutions are addressed in detail in the second section of this paper: "Information Sharing Across Critical Communities." While reaching out to these institutions, the PM-ISE and ISC must also seek to improve coordination among federal departments and agencies, including the DoD, DHS, CIA, and FBI. Improved coordination across these departments and agencies will enable the federal government to better support the operations of the ISE's SLT participants and integrate information provided by SLT actors into federal processes.

Integration of foreign actors into the ISE likewise involves the development of a culture of collaboration. The Plan contemplates that policies facilitating information sharing with foreign actors will be developed across Phases 1 and 2 and will address such issues as access and control of restricted U.S. or foreign information, maintaining privacy rights of U.S. citizens, and ensuring the quality and timeliness of data exchanged with foreign partners. These policies will also assist U.S. agencies in understanding domestic practices of foreign governments and will enable them to develop a framework for international terrorism information exchange. According to the Plan, the Foreign Government Information Sharing Working Group, a body created by the State Department in November 2005, will provide recommendations on privacy issues, assist in the negotiation of international agreements facilitating information sharing, and work with the PM-ISE to compile "best practices" on terrorism information sharing with foreign partners. The Plan also requires the ISC to develop common policies for the handling electronic foreign information.

As for non-government actors, the Plan stresses that data exchange with private entities involve the development of a "robust" cross-sector public/private partnership. The central aim of information sharing between government and private sector actors in the ISE is to protect the nation's critical infrastructure. The Plan notes, "The private sector understands its processes, assets, and operations best and can be relied upon to provide the required private sector subject matter expertise." Improved cross-sector sharing will require standardizing threat alerts and notifications and ensur-

65 *ISE Implementation Plan, supra* note 24.
66 *Ibid*.
67 *Ibid*.

ing the rapid exchange of information between businesses and government on "incidents…and vulnerabilities" relevant to securing the nation's critical infrastructure.

The Plan urges that the Private Sector Subcommittee of the ISC develop a plan for public/private sector sharing that encourages participants to develop trust, build strong relationships, and implement a culture of mutual sharing. In the course of its work, the Private Sector Subcommittee will be guided by the President's standards and policies on the protection of privacy in the ISE.[68]

Challenges to Implementing the ISE

While setting forth strategies to organize and direct the establishment of the ISE, the Plan also discusses challenges to creating an environment of robust information exchange. Advancing a culture of sharing, protecting privacy and civil liberties, and reforming security clearance procedures, are identified as key areas of difficulty in implementing the ISE. In general, challenges to implementing the ISE tend to stem from the tension between the value of information sharing and the need to ensure data security.

The Plan acknowledges that cultivating a willingness to share and creating favorable perceptions of ISE policies will require proactive efforts on the part of the PM-ISE, the ISC, and the internal staffs of ISE participants. As a first step, departments and agencies that comprise the ISC have each selected a senior official that will supervise efforts to implement the ISE within their respective entities. The Plan urges that these officials collaborate closely with the PM-ISE and the ISC to "develop high-level information sharing performance measures" and provide the DNI with an annual assessment report.

The Plan also offers several practical strategies on transforming a "need to know" culture into a "need to share" environment. The Plan stresses the importance of training initiatives (both "core" training programs on common policies established across the ISE as well as programs specific to a department or agency's function in the ISE), the development of monetary and non-monetary incentives to share information, and the acknowledgment of individuals who advance information sharing within their department or agency. The Plan recommends that ISE participants circulate bulletins among their staffs detailing concrete benefits gained by sharing initiatives and compile information on "best practices." Additionally, the Plan suggests that an annual Federal award be offered to the department or agency that has best cultivated a culture of sharing. To eliminate disincentives to information sharing, the Plan reminds federal ISE participants that the President has authorized them to notify the Attorney General and DNI of legal restrictions, not required to protect civil liberties, which obstruct information sharing. Upon such a notification, the Attorney General and DNI may recommend specific changes to the Assistant to the President for Homeland Security and Counterterrorism (APHS-CT), the Assistant to the President for National Security Affairs (APNSA), and the Director of OMB for their review.[69]

On privacy and civil liberties, the Plan affirms that implementation of the ISE will stress the importance of constitutional and other legal restrictions on participants' access, control, and use of shared data. The Plan expects federal ISE participants to identify the legal requirements that specifically pertain to information they seek to transmit or receive in the ISE. It also reminds them of their responsibility to fully implement the ISE Privacy Guidelines, which are discussed in detail in the portion of this paper entitled, "Protecting Privacy and Civil Liberties." Finally, the Plan recommends that federal ISE participants offer training on privacy procedures and foster public awareness of the legal restrictions that guide their use of information in the ISE.

68 *Ibid.*

69 *Ibid.*

Another major challenge to the success of information sharing policies involves the reform of security clearance procedures. The Plan provides an overview of efforts to initiate reform and urges that agencies work together to develop standardized certification and accreditation policies. The Plan also notes that in Executive Order 13381, *Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information*, the President has delegated authority to the Office of Management and Budget (OMB) "for the government-wide initiative to make clearance processes uniform, centralized, efficient, timely and reciprocal." Though the Office of Personnel Management (OPM) is creating a cross-agency security clearance database and the ODNI is issuing recommendations to facilitate rapid reform, the Plan urges that the PM-ISE and the ISC to supervise and assess both reform processes and ISE participants' compliance with them.[70]

Assessment and Criticism

With the resignation of former PM-ISE John Russack, issuance of the Implementation Plan had been delayed. However, when Negroponte delivered PM-ISE McNamara's Implementation Plan to Congress in November 2006, the response was largely positive. John Negroponte, then DNI, recognized McNamara's hard work in producing the Plan and emphasized the Plan's significance.[71] Similarly, in January 25, 2007, Charles E. Allen, Assistant Secretary for Intelligence and Analysis at the Department of Homeland Security, told Congress that the Plan reflects a "coordinated approach" that should lead to "improved flow of internal information, reduced redundancy and overlapping activities, and improved collaboration with the members to ensure that the Information Sharing Environment supports DHS' missions and requirements."[72]

The Plan was also lauded as a "major step forward"[73] in the incremental process of realizing the recommendations set forth by the 9/11 Commission. The Plan's timetable, which requires Phase 2 implementation actions to be completed by 2009, is a benchmark that many ISE participants consider ambitious, but reachable.[74] Phase 1 was due for completion in June 2007, though the PM-ISE has yet to issue a report assessing the success of this implementation phase.

The Plan has generally been commended for providing the broad strategies necessary for successful ISE implementation but has received some criticism for not adequately addressing the needs of SLT government and law enforcement officials. Though the International Association of Chiefs of Police notified Congress that it "strongly supports the Plan" and is "particularly pleased that the ISE plan emphasizes the vital role"[75] of law enforcement officers, others have asserted that the Plan does not effectively coordinate federal and SLT information sharing. Critics complain that the Plan fails to emphasize the need for federal officials to pay careful attention to the content and format of the information they provide to SLT partners.[76] Furthermore, SLT participants have encountered both technical challenges and difficulties in deciphering their roles and responsibilities in the ISE vis-à-vis federal entities.[77] Slade Gorton, a former 9/11 Commissioner, testified before Congress on January 9, 2007, stating, "We continue to hear about turf fights about who is in charge of information sharing with state and local governments. We continue to hear complaints from state and local officials about the quality of the information they

70 *Ibid.*

71 *Information Sharing Environment Implementation Plan Report Sent to Congress, supra* note 49.

72 *Intelligence Revision*, CQ Congressional Testimony, Jan. 25, 2007 [hereinafter *Intelligence Revision*].

73 *Implementing Recommendations, supra* note 55.

74 *Ensuring Full Implementation of the 9/11 Commission's Recommendations*, CQ Congressional Testimony, Jan. 9, 2007 [hereinafter *Ensuring Full Implementation*].

75 *Ibid.*

76 *Ibid.*

77 Stew Magnuson, *Local's Role in Intelligence Sharing Pondered*, National Defense, June 1, 2006 [hereinafter Magnuson].

receive. Suffice it to say many questions and issues remain about the implementation plan for the information-sharing environment. The problem with information sharing is far from resolved.[78]"

Legal Framework of the ISE

The impetus for the IRTPA's creation of the ISE may be traced to the 9/*11 Commission Report*, which offered a detailed analysis of how the lack of information sharing contributed to the government's failures in the period leading up to the September 11th attacks. While the dominance of a "need-to-know" culture had greatly influenced information decision-making prior to September 2001, the 9/11 Commission pointed out that the application of Department of Justice procedures under the Clinton administration had also obstructed information sharing.[79] Because of suspicions of inappropriate use of Foreign Intelligence Surveillance Act (FISA) warrants, then Attorney General Janet Reno had devised information sharing policies that heavily regulated the exchange of information between the intelligence and law enforcement communities. These procedures had the effect of reducing information sharing to such a degree that they eventually earned the epithet, "the Wall."[80]

According to the report, other factors also contributed to this perception, for example, a perceived lack of enthusiasm for information sharing on the part of the Office of Intelligence Policy Review and Foreign Intelligence Surveillance Court created the perception that exchanging data between intelligence and criminal investigators was, if not forbidden, than at least very discouraged. The National Security Agency (NSA) likewise hindered sharing through its reluctance to exchange information on Osama bin Laden with prosecutors. When the September 11th attacks occurred, a persistent lack of information sharing prevented personnel of the New York Office of Emergency Management (OEM), the Fire Department of New York (FDNY), the New York Police Department (NYPD), and the Port Authority Police Department (PAPD) from coordinating a unified response.[81]

In response to these observations, the 9/11 Commission recognized that effective information sharing would require unity of effort. It therefore recommended that the president, being in the optimal position to initiate government-wide change, guide the development of robust information sharing practices. The 9/11 Commission further acknowledged, as has current PM-ISE McNamara, that developing information sharing strategies, rather than implementing technological changes, will constitute the primary challenge of reforming information handling practices. The Commission wrote, "Despite the problems that technology creates, Americans' love affair with it leads them to also regard it as the solution. But technology produces its best results when an organization has the doctrine, structure, and incentives to exploit it."

Information sharing legislation enacted following the 9/11 attacks attempts to dismantle Cold War "need to know" mentalities and coordinate interagency communications. The legal framework of the ISE incentivizes sharing and heeds the 9/11 Commission's recommendation that "intelligence gathered about transnational terrorism…be processed, turned into reports, and distributed" to appropriate federal, foreign, SLT, and private sector actors, no matter where the information is initially collected.

The USA PATRIOT Act

The USA PATRIOT Act made an early attempt to improve information sharing by deconstructing barriers between the intelligence and law enforcement communities. Recognizing that the nation's security is jeopardized when officials across fed-

78 *Ensuring Full Implementation, supra* note 74.
79 National Commission on Terrorist Attacks, *supra* note 1.
80 *Ibid.*
81 *Ibid.*

eral departments and agencies fail to collaborate effectively on terrorism issues, the framers of the legislation sought to mitigate tendencies to sharply divide criminal investigations from intelligence collection and analysis missions.

Section 203 of the Act, which addresses "authority to share criminal investigative information," amends the Federal Rules of Criminal Procedure to permit the sharing of grand jury information involving "foreign intelligence," "counterintelligence," or "foreign intelligence information."[82] Federal persons authorized to receive grand jury information under the Act represent a variety of relevant communities, including law enforcement, intelligence, immigration, national defense, and national security.[83] Shared information may likewise derive from diverse collection techniques, as the Act permits the exchange of electronic, wire, and oral interception data.[84]

The USA PATRIOT Act bridges gaps between law enforcement and intelligence officials by also amending relevant provisions of the National Security Act of 1947. In section 905, the Act requires that the Attorney General and heads of other federal law enforcement agencies provide the Director of Central Intelligence with foreign intelligence information acquired in the course of criminal investigations.[85] To avoid ambiguity and overcome the perceptions that had discouraged sharing between law enforcement and intelligence officials prior to 9/11, the Act explicitly invokes the definitions of "foreign intelligence" and "counterintelligence" contained in the National Security Act of 1947 and carefully defines "foreign intelligence information."

Because the USA PATRIOT Act attempts to effect cultural change, the Attorney General and Director of Central Intelligence must collaborate to implement its provisions.[86] These officials must develop information disclosure guidelines and ensure that relevant agencies provide training opportunities that stress procedures for identifying and exchanging foreign intelligence information.[87] According to section 908 of the Act, training programs should address both horizontal and vertical sharing practices by targeting federal officials not accustomed to handling foreign intelligence information as well as SLT officials likely to encounter foreign intelligence information in the course of their daily operations or in the event of a terrorist attack.[88]

The USA PATRIOT Act sets the stage for increased sharing initiatives by not only deconstructing "the Wall" between the law enforcement and intelligence communities but also by improving coordination among federal agencies with counter-terrorism functions. For example, the Act's amendments to section 106 of the Foreign Intelligence Surveillance Act of 1978 (FISA) encourage federal officers conducting electronic surveillance to "consult with federal law enforcement officers" and synchronize their "efforts to investigate or protect against" national security threats.[89] In particular, the Act emphasizes the need for increased coordination in response to threats emanating from foreign powers, international terrorism, and clandestine intelligence activities.

Though enacted rapidly after the 9/11 attacks, the USA PATRIOT Act provides an important underpinning for the ISE by addressing the critical role of non-federal actors in ensuring the nation's security. In addition to mandating that training opportunities be extended to SLT officials, the Act recognizes the importance of local law enforcement officers in protecting critical infrastructure and investigating acts of domestic terrorism. By recognizing that the investigation of "terrorist conspiracies and activities" will often be "multi-

82 *See* Fed. R. Crim. P. 6(e)(3)(C).
83 *Ibid.*
84 *Ibid.*
85 *See* 50 U.S.C. § 403-5(b).
86 *See* 28 U.S.C. § 509.
87 *Ibid.*
88 *Ibid.*
89 *See* 50 U.S.C. § 1806.

jurisdictional" in nature, the USA PATRIOT Act encourages active cooperation among federal and SLT entities that have since been integrated into the ISE.[90]

Homeland Security Act (HSA) of 2002

The Homeland Security Act (HSA) of 2002 builds upon sharing opportunities contained in the USA PATRIOT Act by integrating the newly created Department of Homeland Security (DHS) into the community of law enforcement and intelligence officials permitted or directed to exchange information under the USA PATRIOT Act. In section 202, the HSA ensures that DHS is included in existing sharing practices by requiring that the DHS Secretary has access "to all information…relating to threats of terrorism against the United States," including data concerning "infrastructure" and other homeland "vulnerabilities."[91] Because of the urgency with which DHS needed to begin its operations, the HSA urged that shared information include data in a variety of formats, such as, "reports, assessments, [and] analyses." Furthermore, the HSA specified that sharing with DHS should occur irrespective of which agency initially collected or prepared the information to be shared or "whether…such information has been analyzed." The ISE would later refine attempts to share high volumes of information by requiring that participating departments and agencies establish appropriate data quality control policies.

To ensure that information exchange practices endure, the HSA calls for the DHS Secretary and other department and agency heads to develop sharing policies such that DHS receive homeland security information from other agencies "on a regular or routine basis." Section 202(d)(2), for example, requires the DHS Secretary and the Director of Central Intelligence to jointly develop policies for sharing across the homeland security and intelligence communities. Before the ISE could develop communications pathways for sustained vertical sharing, these elements of the HSA encouraged coordination and effective response to threats or attacks on critical infrastructure.

The content of the HSA that most foreshadows the goals of the ISE is section 892 on "facilitating homeland security information sharing procedures."[92] Like the IRTPA, section 892 contemplates unified guidance of sharing procedures by requiring the President to prescribe and implement procedures under which federal agencies can share homeland security information with other federal partners, as well as with appropriate state and local personnel. The President's responsibilities include delineating procedures for the sharing and handling of both classified and sensitive but unclassified information across interagency lines. Federal agencies have the reciprocal duty of designating an individual to manage the implementation of the President's procedures.[93]

Since section 892 directs that the President's policies "apply to all agencies of the Federal Government," it represents significant step toward Congress' 2004 decision to establish a government-wide information sharing environment. However, unlike the ISE, which concentrates on the development of sharing strategies and a government-wide policy "approach," the HSA emphasizes the creation of sharing "systems," which may be too restrictive to effect long-term cultural change. Section 892, for example, requires federal agencies and appropriate state and local officials to share homeland security information systems that can exclude users on the basis of "geographic location," "type of organization," "position" or "need to know." The ISE later improved upon the HSA by launching an effort to replace "need to know" with "need to share." By incorporating "need to know" criteria into the establishment of information sharing systems, section 892 of the

90 *See* 42 U.S.C. § 3796(h).

91 Homeland Security Act of 2002, 6 U.S.C. § 122 (2002).

92 6 U.S.C. § 482.

93 *Ibid.*

HSA does little to reform the culture that hinders sharing.

Executive Order 13311 Homeland Security Information Sharing

This order delegates much of the President's authority under sections 892 and 893 of the Homeland Security Act of 2002 to the Secretary of Homeland Security. Thus, the Secretary assumes responsibility for developing and implementing homeland security information sharing procedures between federal departments and agencies as well as state and local officials. Consistent with the Act, these procedures must include mechanisms for identifying and maintaining the security of sensitive and classified information. However, the order indicates that the Secretary's procedures remain subject to exceptions made by the President or an official to whom he delegates this responsibility.

To develop the sharing procedures, the President directs the Secretary of Homeland Security to collaborate with other officials, including the "Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Energy, the Director of the Office of Management and Budget, the Director of Central Intelligence, [and] the Archivist of the United States."[94] The President also permits the Secretary of Homeland Security to consult other federal officials that the Secretary deems could provide proper assistance to his efforts to carry out the mandate of section 892 of the HSA.

The President retains, however, his authority under sections 892(a)(2) and 892(b)(7) under the Act.[95] Section 892(a)(2) authorizes him to see that homeland security information sharing procedures apply to all federal agencies.[96] Under section 892(b)(7), the President must identify federal agencies to evaluate homeland security information being shared and synthesize such data with intelligence information.[97]

Executive Order 13356 Strengthening the Sharing of Terrorism Information to Protect Americans

Executive Order 13356 guides federal agencies' efforts to develop and improve information sharing by mandating that they concentrate on four priorities: (1) the "detection, prevention, disruption, preemption, and mitigation of terrorist activities" against the United States; (2) the effective sharing of terrorism information across federal agencies; (3) the successful integration of SLT entities into sharing initiatives; and (4) the continued acquisition of terrorism information.[98] The President reminds federal agencies that these tasks shall be accomplished while safeguarding Americans' privacy and civil liberties.

To achieve these goals, E.O. 13356 requires heads of federal agencies that "possess or acquire terrorism information" to rapidly share such data with heads of agencies responsible for "counterterrorism functions." Additionally, the President instructs the Director of Central Intelligence to cooperate with the Attorney General and other agency heads in developing common sharing procedures. According to E.O. 13356, the procedures should aim to mitigate obstacles to sharing caused by the information classification system. For example, the President states that agencies should "creat[e] unclassified versions [of terrorism information] for distribution whenever possible." The Director of Central Intelligence and Attorney General's procedures should also address civil liberties concerns by stipulating in "clear, understandable, consistent, effective, and lawful" terms how information, once collected, is to be used, disseminated, and stored.[99]

94 Exec. Order No. 1331, 68 Fed. Reg. 147 (July 31, 2003).
95 *Ibid.*
96 *See* 6 U.S.C. § 42.
97 *Ibid.*
98 Exec. Order No. 13356, 69 Federal Register 169 (September 1, 2004).
99 *Ibid.*

The President recognizes that greater unity of effort is required for effective information sharing and in section five of his order, mandates the establishment of an Information Systems Council. The Council's principal obligation is to develop, within 120 days, a plan for creating an "interoperable terrorism information sharing environment."[100] Serving as a prelude to establishment of the ISE by the IRTPA four months later, this plan describes the "functions, capabilities, and resources" of an interoperable terrorism information sharing environment, identifies challenges to its implementation, and suggests feasible short-term solutions. The Council is also directed to propose strategies on how state and local authorities may be integrated into the environment and to recommend ways in which the "interoperable" environment could be transformed into a fully operational ISE.[101]

Intelligence Reform and Terrorism Prevention Act of 2004

The IRTPA mandates an even more extensive information sharing regime than either the USA PATRIOT Act or the Homeland Security Act of 2002. The legislation establishes and provides the principal management architecture for the endeavor now referred to as the Information Sharing Environment (ISE). Though neither the USA PATRIOT Act nor the HSA promoted sharing through an "information environment," both acts worked toward integrating information policies across the intelligence, law enforcement, and homeland security communities. By encouraging horizontal cooperation across federal agencies and vertical cooperation between federal and SLT officials, the USA PATRIOT Act and HSA provided a foundation for the IRTPA's creation of a government-wide sharing initiative.

Under section 1016(b)(1) of the IRTPA, the President must facilitate the sharing of "terrorism information" by establishing an ISE that combines policies, procedures, and technologies linking people, systems, and information among all federal, state, local, and tribal entities, as well as the private sector.[102] The President must also ensure protection of privacy and civil liberties in promulgating information sharing procedures. "Terrorism information" shared throughout the ISE refers not only to intelligence, law enforcement, military, and homeland security information, but also to any information relevant to individuals or groups involved in the "existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support or communications" of transnational terrorism. Though the IRTPA does not address the establishment of common quality control procedures, it does require that information shared through the ISE be accessible "in a form and manner that facilitates its use in analysis, investigations and operations."[103]

The IRTPA recognizes the practical difficulties of information sharing and therefore requires participating departments and agencies to develop and maintain electronic directory services for locating people, organizations, and locations connected by the ISE. Unlike the HSA's reliance on information systems, however, the IRTPA clarifies that the ISE will be created through the use of both "policy guidelines and technologies." The framers of the IRTPA echoed the 9/11 Commission's warning that improved information technology alone is not sufficient to advance the nation's anti-terrorism efforts. Rather, as the IRTPA states, the ISE, while protecting information security, must succeed in managing "access to data rather than just systems and networks."[104]

One weakness of the statute is its lack of specificity in discussing several key issues on ISE establishment. For example, in section 1016(b)(2)(B), the Act requires that the ISE "incorporate strong

100 *Ibid.*
101 *Ibid.*
102 6 U.S.C. § 485, *supra* note 14.
103 *Ibid.*
104 *Ibid.*

mechanisms to enhance accountability and facilitate oversight." The use of the relative term "strong mechanisms" does not appear to provide an adequately clear benchmark for assessing the effectiveness of the executive branch's efforts. Similarly, as earlier noted, the statute fails to designate the official to whom the program manager reports and only briefly mentions his budget, a significant factor affecting the extent of the program manager's involvement in ISE implementation.

However, the IRTPA greatly advances information sharing by creating a coordinated "environment," rather than simply adding to the list of sharing responsibilities stipulated by the USA PATRIOT Act and the HSA. The information sharing initiative set forth by the IRTPA capitalizes on existing sharing capabilities and allows ISE participants "direct and continuous" access to information so as to establish a sharing environment in which there are "no single points of failure."

Presidential Memorandum on Strengthening Information Sharing, Access, and Integration—Organizational Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment

This memorandum resolves the IRTPA's ambiguity regarding the program manager's authority by following the recommendation of the Commission on Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction that the PM-ISE be designated as part of the Office of the Director of National Intelligence (ODNI). The change empowers the DNI to "exercise authority, direction, and control" over the PM-ISE and ensure that the PM-ISE fulfills his responsibilities under section 1016 of the IRTPA effectively and in accordance with the President's directions.[105]

Though the memorandum clarifies the issue of authority over the PM-ISE, it raises the question of whether the DNI is the appropriate official to fulfill this function. The President's decision is logical given the DNI's roles and responsibilities, as the Commission on Weapons of Mass Destruction recognized. However, there is a concern that requiring the DNI to perform an oversight role in the process of establishing the ISE may detract him from his duties of coordinating activities of intelligence community.

Executive Order 13388 Further Strengthening the Sharing of Terrorism Information to Protect Americans

Executive Order 13388 represents in large part an updated version of the President's directions in E.O. 13356, which is officially revoked by E.O. 13388. While acknowledging the advances in terrorism information sharing set in motion by the enactment of the IRTPA in December 2004, E.O. 13388 repeats many of the policy goals listed in E.O. 13356. The President revises his previous directions by requiring that the "common standards" on information sharing being developed by the Director of Central Intelligence and the Attorney General in response to E.O. 13356 concentrate on facilitating implementation of the ISE.[106] The President's order also establishes the Information Sharing Council, the advisory body whose mission, as previously discussed, involves collaborating with the program manager and guiding implementation of the ISE.[107]

Presidential Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment

This memorandum directs establishment of the ISE by issuing instructions for the PM-ISE as well as five ISE implementation guidelines. The PM-ISE is to assess the needs and information shar-

105 Memorandum on Strengthening Information Sharing, *supra* note 28.

106 Exec. Order No. 13388, 70 Federal Register 62023 (Oct. 27, 2005).

107 *Ibid*.

ing capabilities of ISE participants. He must consult with the Information Sharing Council (ISC) in preparing, within 90 days, a report on federal departments and agencies' information sharing resources.[108] This assessment is intended to enable the ISE to "leverag[e]" and enhance existing information sharing policies, resources, and technological capabilities. Then, the PM-ISE must supplement his assessment of information sharing resources by collaborating with the Director of the National Counterterrorism Center (NCTC) to report on the needs and missions of ISE participants with "counterterrorism responsibilities." When this information is compiled and analyzed, the DNI must direct the PM-ISE to work with the ISC to develop strategies, policies, and procedures to implement the ISE.[109]

After discussing the PM-ISE's duties, the President provides five guidelines for ISE implementation, consistent with his responsibilities under section 1016(d) of the IRTPA. First, the President emphasizes the need for creating "common standards" for information collection, access, sharing, and use within the ISE. The President directs the DNI to collaborate with the Attorney General and the Secretaries of State, Defense, and Homeland Security to create these information handling policies.

Second, the President states that SLT and private sector officials must "have the opportunity to participate as full partners in the ISE." He therefore designates the Secretary of Homeland Security and the Attorney General to collaborate with the Secretaries of State, Defense, Health and Human Services, and the DNI to establish a "common framework" describing the roles and responsibilities of ISE participants.

Third, the President recognizes that effective information sharing will require the development of procedures to homogenize various departments and agencies' policies on handling and sharing Sensitive But Unclassified (SBU) information. While ensuring that sufficient security is provided for shared information, the Secretary of Homeland Security and the Attorney General, in cooperation with the Secretaries of State, Defense, Energy, and the DNI, must submit recommendations on the "the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information."

Fourth, the President orders the Secretary of State to work with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, as well as the Attorney General and the DNI, to develop procedures enabling effective information sharing between executive departments and foreign allies. These procedures must facilitate "international access and exchange" and provide consistent practices for handling information received from foreign governments.

Fifth, the President affirms the federal government's "solemn obligation…to protect the legal rights of all Americans in the effective performance of national security and homeland security functions." He requires the Attorney General and the DNI to develop ISE privacy guidelines. Furthermore, he instructs the heads of federal ISE participants to "ensure on an ongoing basis" that "personnel, structures, training, and technologies are in place" to protect privacy rights and that the guidelines developed by the Attorney General and the DNI are fully implemented.

The President concludes his memorandum in emphasizing the importance of establishing a "need to share" culture throughout the ISE. He directs that executive departments and agencies prepare for ISE participation by developing information sharing accountability procedures, dismantling policies that discourage sharing, and allocating personnel and resources to the goal of advancing

108 Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment, PUB. PAPERS, Dec. 26, 2005.

109 *Ibid*.

terrorism information sharing.[110] Furthermore, he directs that senior officials be appointed by participating departments and agencies to oversee information sharing within their respective offices and work closely with the PM-ISE and ISC in implementing the ISE. These officials will provide annual information sharing assessments to the DNI as well as notify the Attorney General of any specific legal requirements that should be reviewed because of their effect of obstructing information sharing.[111]

Protecting Privacy and Civil Liberties

Section 1016 of the IRTPA and E.O. 13388 treat the goals of improved information sharing and privacy protection as twin aims of the ISE. Rather than representing increased security and the protection of legal rights as mutually exclusive goals, the legal underpinning of the ISE takes the position that both goals can be reconciled within the framework of the ISE. Relevant law suggests that implementation of the ISE should create a "culture of privacy,"[112] while fostering a "culture of sharing," in order to strike an appropriate balance between security and privacy needs.

The procedures for establishing the ISE therefore offer both a strategy and structure for protecting privacy and civil liberties. Pursuant to the December 2005 Presidential Memorandum on the Guidelines and Requirements in Support of the Information Sharing Environment, the Attorney General and Director of National Intelligence (DNI) established the President's Information Sharing Environment Guideline 5 Working Group, which consisted of privacy officials of the ISE's participating departments and agencies. The working group's task was to assess the privacy and civil liberties implications of existing information sharing procedures and then to develop guidelines for continued protection of legal rights as information is collected, used, shared, and stored by ISE participants.

Sharing Information While Safeguarding Legal Rights

In December 2006, the President approved the working group's *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (Guidelines). The ISE Privacy Guidelines treat as "protected information" data about U.S. citizens or lawful permanent residents subject to privacy or other legal restrictions under the U.S. Constitution and federal law, or specifically designated by executive orders or international agreements.[113] Though the Guidelines apply only to federal entities, they require that federal participants in the ISE collaborate with information sharing partners in SLT and foreign governments, as well as the private sector, to "develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines." The Guidelines also contemplate that the public will act as a check on information sharing activities and therefore encourage public awareness of the ISE and relevant privacy restrictions.

The Guidelines stress that the ISE comply with all existing legal restrictions on protected information and remind participants that personally identifiable information may be distributed through the ISE only if it meets the definition of terrorism information, homeland security information, or law enforcement information as specified in section 1016 of the IRTPA and section 482(f) of the Homeland Security Act of 2002. Participating agencies are therefore directed to review data it

110 *Ibid*.

111 *Ibid*.

112 *Protection of Privacy*, CQ Congressional Testimony, Apr. 6, 2006.

113 *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*, Dec. 2006, available at http://ise.gov/docs/ise%20privacy%20guidelines%2012-4-06.pdf [hereinafter *Guidelines to Ensure that the Information Privacy*].

intends to share through the ISE for classification as "protected information," as well as relevant law, on a continual basis. Agencies must develop internal procedures for monitoring compliance with legal restrictions on the information it accesses, shares, or stores as a result of its participation in the ISE. To facilitate the sharing process and ensure that personally identifiable information receives continued protection as it is shared and used in the ISE, the Guidelines call for each agency to develop a system for informing ISE partners when shared information falls within the category of "protected information" or is subject to particular legal restrictions.

While offering necessary guidance on compliance with existing legal requirements, the Guidelines provide additional measures to protect privacy and civil liberties. The Guidelines emphasize information security by requiring ISE participants to take appropriate "physical, technical, and administrative" measures to safeguard against inappropriate access, use or distribution of protected information in the ISE. To prevent the use or sharing of erroneous data, the Guidelines stipulate that agencies develop procedures to minimize error, promptly correct erroneous information, and notify ISE participants when errors do occur.

As an added safeguard, agencies are required to exercise care when synthesizing information about an individual from several sources and are instructed to "retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use." Furthermore, any protected information shared through the ISE later determined not to meet the statutory requirements of "terrorism information," "homeland security information," or "law enforcement information" must be promptly deleted.

Enforcement mechanisms for privacy policies are also addressed by the Guidelines, which require that agencies participating in the ISE appoint at least one senior official as an ISE privacy official, with the responsibility of overseeing, enforcing, and updating their respective agencies' procedures for complying with the Guidelines. Privacy officials are additionally directed to see that its agency offers training on ISE privacy policies, as well as "consider[s] and implement[s], as appropriate, privacy enhancing technologies." Agencies should supplement the efforts of its privacy officials by developing policies that ensure accountability, provide for timely and appropriate investigations of possible privacy violations, and implement mechanisms to redress complaints from individuals.

Finally, the ISE provides a governance structure for managing privacy policies. Pursuant to the Guidelines, the PM-ISE established a standing ISE Privacy Guidelines Committee on December 4, 2006.[114] The Committee consists of privacy officials of the departments and agencies that comprise the Information Sharing Council (ISC).[115] Co-chaired by Alexander Joel, the ODNI's Civil Liberties Protection Officer, and Jane Horvath, Privacy and Civil Liberties Officer of the Department of Justice,[116] the ISE Privacy Guidelines Committee supervises implementation of the Guidelines, ensures uniformity in the application of the Guidelines across agencies, highlights "best practices," and serves as "a forum for resolving issues on an inter-agency basis."[117]

The ISE Privacy Guidelines Committee is assisted by the Privacy and Civil Liberties Oversight Board (PCLOB), which was created by section 1061 of the IRTPA pursuant to a recommendation by the 9/11 Commission. The PCLOB is autho-

114 *Program Manager for the Information Sharing Environment Releases Privacy Guidelines*, US Newswire, Dec. 4, 2006 [hereinafter *Privacy Guidelines*].

115 *Guidelines to Ensure that the Information Privacy, supra* note 113.

116 *Privacy Guidelines, supra* note 114.

117 *Guidelines to Ensure that the Information Privacy, supra* note 113.

rized to review and provide guidance on a variety of policies designed to enhance the nation's security against the threat of terrorism, including information sharing.[118] Consisting of five presidential appointees,[119] the Board held its first meeting on March 14, 2006, and is working to provide the President and the heads of executive departments and agencies with appropriate recommendations to ensure that privacy and civil liberties are adequately protected within the ISE.[120]

The ISE Privacy Guidelines are intended to enable ISE participants to develop privacy procedures best suited to their respective missions. However, the Guidelines also seek to ensure consistency in the application of legal requirements and uniformity in the oversight of information sharing activities. As Horvath and Joel remarked in the "Introduction to the ISE Privacy Guidelines," "[T]he ISE Privacy Guidelines strike a balance between consistency and customization, substance and procedure, oversight and flexibility."[121]

Concerns Remain

Despite efforts to ensure that the protection of privacy and civil liberties is, as McNamara has stated, "a core tenet of the ISE,"[122] concerns linger about the extent and adequacy of the protections provided. Civil liberties advocates and members of Congress have been vocal in criticizing the ISE Privacy Guidelines as providing only minimal guidance. Critics contend that protecting privacy has not been adequately emphasized as information sharing policies are implemented and claim that the Guidelines, though attractive on paper, are flawed in practice.

The existence of improved and more powerful information technology has consistently caused worry about federal capabilities for accessing, using, and storing personally identifiable information. The implementation of the ISE heightens these concerns by facilitating the dissemination of protected information and increasing the likelihood that attempts to synthesize information from numerous sources will result in errors with implications for individual rights. In addition, many agree with the 9/11 Commission's observation that the sense of heightened urgency on security matters prompted by the nation's experience on September 11, 2001 could jeopardize civil liberties over the long haul.

Before the ISE Privacy Guidelines had been drafted, Benjamin Powell, general counsel for the DNI, had been tasked with reviewing legal restrictions on the federal government's access, use, and dissemination of information as of July 2005. Concerns that privacy and other civil liberties would be overlooked in the effort to maximize the value of information for security purposes arose when Powell's work was to be carried out confidentially.[123] Additionally, at his confirmation hearings, Powell had been instructed by some members of the Senate Select Committee on Intelligence to distinguish, as precisely as possible, true legal requirements from prudential, but not legally mandated, practices to preserve privacy and other legal rights.[124]

Republican Senator Pat Roberts of Kansas told Powell to avoid "overly cautious and inaccurate interpretations" of restrictions on information handling and urged, "I expect the lawyers of the intelligence community—along with its analysts and operators—to step right up to those lines [of what is legally permissible]. Don't go over them, but step up to them."[125] Roberts's view caused ample

118 *See* 6 U.S.C. § 485.

119 *Balancing Civil Liberties and National Security Needs*, CQ Congressional Testimony, June 6, 2006 [hereinafter *Balancing Civil Liberties*].

120 *Ibid.*

121 Joel, Alexander & Jane Horvath, *An Introduction to the ISE Privacy Guidelines*, Dec. 2006, available at http://ise.gov/docs/ise%20privacy%20guidelines%20intro%20-rev.pdf.

122 *Privacy Guidelines, supra* note 114.

123 Shaun Waterman, *Intelligence Chief to Review Privacy Rules*, UPI, July 25, 2005 [hereinafter Waterman, *Intelligence*].

124 *Ibid.*

125 *Ibid.*

anxiety among civil libertarians, who argued that the line separating permissible from impressible behavior is not clearly visible. They also claimed that comfortableness with minor legal violations could lead to increased and more alarming violations in future security practices.

Powell, however, resolved to determine the "proper balance between the national interest in the collection, dissemination, and maintenance of intelligence, and the national interest in protecting the legal rights of all US persons" and pointed out that that much of the law he had been asked to review dated to the Reagan administration. Legal opinions lingering from the 1980s, he stated, are not necessarily compatible with efforts to manage current national security threats. In addition, Powell commented on the importance of enabling privacy law to "keep[] pace with current technology" and changes within agencies that perform national security functions, such as "the continuing transformation of the CIA and FBI." He explained that updating privacy would ensure that "appropriate safeguards are put in place during this transformation."[126]

Though the Privacy and Civil Liberties Oversight Board (PCLOB) was intended to provide a competent mechanism for protecting individual rights while the federal government intensifies national security measures, members of Congress and civil liberties activists have claimed that creation of the PCLOB had not been treated as a priority by the Bush administration. In December 2005, a congressional reported card gave the administration a grade of "D" under the two categories of "Civil Liberties and Executive Power" and "Privacy and Civil Liberties Oversight Board."[127] Though Congress gave the grade of "B" under the category "Balance Between National Security and Civil Liberties," it expressed concern that establishment of the PCLOB and appointment of its five members had been unreasonably slow, suggesting that the PCLOB was of little import to the executive branch.[128] According to Representative Christopher Shays, the process of establishing the board took more than 15 months and the Board has since "had to struggle with issues of budget, staff support, [and] office space."[129]

Criticism of the Board extends to its functions and powers, which some claim are inadequate given the body's purpose of overseeing implementation of the ISE as well as other security measures taken to protect the nation against terrorism. Unlike some original proposals for legislation on intelligence reform, the IRTPA did not provide the Board with subpoena power.[130] Some civil liberties advocates have concluded that the PCLOB cannot offer competent oversight so long as it lacks the power to compel agencies participating in the ISE to provide witnesses or relevant information. They also contend that the PCLOB's lack of subpoena power is exacerbated by the Attorney General's ability to veto certain Board requests for information.[131] The *Los Angeles Times* went so far as to refer to PCLOB as a "paper tiger."[132]

Presidential approval and incremental implementation of the ISE Privacy Guidelines have also not alleviated concerns about privacy and civil liberties in the handling and sharing of terrorism information. The Guidelines, which consist of only nine pages, have been criticized for not providing the level of specificity required to ensure adequate protection of legal rights. In March 2007, Linda D. Koontz, Director of Information Management Issues at the Government Accountability Office (GAO), remarked to the House Subcommittee on Homeland Security that the Guidelines "provide only a high-level framework for ensuring privacy protection and do not address how the collection of information is to be limited."[133]

126 *Ibid.*

127 *9/11 Commission Recommendations: Balancing Civil Liberties and Security*, CQ Congressional Testimony, June 6, 2006.

128 *Ibid.*

129 *Ibid.*

130 *Ibid.*

131 *Ibid.*

132 *Ibid.*

133 *Enhancing Privacy and Civil Rights While Meet-*

Koontz pointed out that the document highlights core values worthy of heightened protection but does not instruct participating agencies on implementing privacy requirements.[134] The Guidelines' reliance on vague language, such as phrases that require agencies to "implement appropriate policies"[135] or "put in place a mechanism"[136] for notifying ISE participants of protected information, provide little assurance of consistency in privacy standards across the ISE's participating communities.

Counter-Arguments and Conclusions

Despite criticism of the Guidelines and the lengthy process of establishing the PCLOB, both the Guidelines and Board do provide a considerable level of protection for legal rights as the ISE is being implemented. Fears that a critical review of privacy laws dating to previous decades threatens civil liberties fail to consider both the changes of U.S. security needs and the federal government's technological capabilities in a post-9/11 world. For instance, both Barry Steinhardt, director of technology and liberty for the American Civil Liberties Union (ACLU) and ODNI General Counsel Benjamin Powell, have expressed the view that privacy law needs to take current technology into account in order to offer effective protection of legal rights.[137]

Though critics correctly point out that the Guidelines were drafted at a level of generality, a highly specific document would not be able to account for the disparate missions of the various agencies participating in the ISE or provide sufficient flexibility for changing information sharing needs. Civil liberties specialists, such as Jane Horvath, Civil Liberties and Protection Officer at the Justice Department, and Alexander Joel, Civil Liberties and Protection Officer at the ODNI, have opined that the Guidelines provide an appropriate foundation for ensuring that specific procedures protecting privacy and other rights are implemented by ISE participants. The two have written, "These government-wide privacy guidelines establish key protections as agencies share information on terrorism…The Guidelines do, in fact, require agencies to establish appropriate redress and transparency mechanisms."[138] Horvath and Joel have also stressed that implementation of the Guidelines will be supervised by both the PCLOB and the ISE Privacy Guidelines Committee, comprised of the privacy officers of each agency participating in the ISE.[139]

It is also worth noting that members of the PCLOB have agreed with Congress's decision not to provide the body with subpoena power in drafting the IRTPA. As Board member Carol E. Dinkins stated to Congress in June 2006, "It is incongruous to even consider an office within the White House requiring subpoena power to compel executive branch agencies or officials to provide it with information."[140] Furthermore, the lengthy process of establishing the Board has been mitigated by its recent progress. According to Dinkins, the Board has established "working relationships" with privacy officials across federal agencies and has also met with many senior officials of agencies participating in the ISE.[141] While the President was not required to appoint a bipartisan membership to the Board, the body has reached out to civil liberties advocates on both sides of the aisle, including such organizations as the American Civil Liberties Union (ACLU), the Center for Democracy an Technology (CDT), the American Conservative Union, and the Markle Foundation.[142]

---

ing Homeland Security Needs, CQ Congressional Testimony, Mar. 21, 2007.

134 *Ibid.*

135 *Guidelines to Ensure that the Information Privacy, supra* note 113.

136 *Ibid.*

137 Waterman, *Intelligence, supra* note 123.

138 Jane Horvath & Alexander Joel, *Editorial—Sharing Necessary Data While Protecting Privacy*, Wash. Post, Dec. 18, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/17/AR2006121700683.html.

139 *Ibid.*

140 *Balancing Civil Liberties, supra* note 119.

141 *Ibid.*

142 *Ibid.*

One remaining problem is that civil liberties advocates, as well as members of Congress, continue to view security and civil liberties as inevitable trade-offs. However, the ISE Privacy Guidelines as PCLOB adopt the refreshing position that enhancing security through increased information sharing need not compromise privacy and other legal rights. As Alexander Joel, Privacy and Civil Liberties Officer of the ODNI remarked, "It is our view that you can do both and you have to do both."[143] Violations of privacy and other legal rights must be addressed with seriousness and consistency, though not at the expense of discouraging activities that will make the nation safer. By increasing information sharing and providing bodies for oversight functions, the structure of the ISE maintains a watchful eye over government activity while also reducing privacy invasions caused by the very threat of terrorist attacks.

II. Information Sharing Across Critical Communities

Defense

The Department of Defense (DoD), whose missions depend upon coordination and agility for success, has taken a natural lead in improving information sharing. The DoD enters the ISE with a sizeable budget and a capacity to conduct sophisticated information technology research. Its experience in synchronizing the needs of military personnel with the capabilities of military intelligence agencies and foreign allies has prepared the Department for the challenges of effective data sharing across participating communities of the ISE.

Military operations in Afghanistan and Iraq have underscored the value of reliable information as a vital asset in the Global War on Terror (GWOT). Coordinating battlefield activity and orchestrating strategies employed by U.S. troops with those of supporting allies depend as heavily upon effective field communication as upon warfighter preparedness and skill. The unique challenges of counter-insurgency operations, as opposed to conventional offensive missions, have also emphasized the need for improved access to information. Increased avenues of communication enable troops to spread information on insurgents' locations and capabilities and enhance awareness of imminent threats.

The "need-to-know" approach to information management, which the ISE is designed to transform into a "need to share" culture, has proven inadequate to support the DoD's operations. Military commanders assert that "stovepipe" systems, where data flows along "top down" vertical pathways on a very limited basis, prevent warfighters from receiving sufficient and reliable data. They also pinpoint inadequate access to information as the cause of a number of tactical errors on the battlefield.[144] "We have bombed things we shouldn't have bombed," Marine Corps Maj. Gen. Michael Ennis, former Defense Intelligence Agency Director for Human Intelligence, has stated frankly.[145] He explained that in certain cases, errors have occurred because information could not be accessed from the databases where it was stored, not because the information had never been acquired[146]. The ability of Northern Command (NORTHCOM) to conduct accurate homeland security missions is also jeopardized by a lack of effective information sharing policies. In the event of a terrorist attack or natural disaster, NORTHCOM would need to collaborate with first responders and other state and local officials that have struggled to obtain requisite clearances for accessing and disseminating information in a restricted "need to know" system.[147]

---

143 Shaun Waterman, *Analysis: DNI Debates Privacy Rule Changes*, UPI, Aug. 21, 2006.

144 Grace Jean, *Information Miscues Lead to Bad Targeting Decisions*, National Defense, Aug. 1, 2006, *available at* http://www.nationaldefensemagazine.org/issues/2006/August/InformationMiscuesLead.htm [hereinafter Jean].

145 *Ibid.*

146 *Ibid.*

147 Press Release, Swan Island Networks, Inc., Swan

John Grimes, DoD Chief Information Officer (CIO) and Assistant Secretary of Defense for Networks and Information Integration, urges that information be "given the same level of emphasis as traditional weapon systems such as guns, tanks, ships and airplanes."[148] He considers access to information critical to success on the ground and has affirmed that "[l]everaging the power of information will provide the agility to deal with uncertainty, make better decisions faster and act sooner."[149] However, the success of military efforts to deploy information as a weapon will hinge upon the federal government's ability to intensify the flow of terrorism and homeland security information to the DoD, as well as to ensure the accuracy and security of shared data. Interagency cooperation through the ISE will therefore comprise a critical component of the DoD's strategy to synthesize information from a multiplicity of sources and provide war-fighters with a more comprehensive understanding of security threats.

Admiral Poindexter's Attempt to Improve Defense Information Capabilities

Before the attacks of September 11, 2001, exposed the need to strengthen security by reforming information policies, the DoD had experimented with programs to enhance data collection and analysis. In 1996, the Pentagon's Defense Advanced Research Projects Agency (DARPA) issued a Broad Agency Announcement (BAA) communicating the DoD's objective of developing technology that would enable the Department to "identify potential future crises and our options for preemption and prevention."[150]

By 1997, Project Genoa had been established to coordinate several DARPA initiatives involving the research and development of sophisticated information technology.[151] Some of the initiatives launched under Project Genoa were aimed at supplementing human analysis capabilities and facilitating information sharing.[152] During the late 1990s, DARPA collaborated with Virginia company Syntek Technologies on Project Genoa, providing an opportunity to Admiral John Poindexter, then Syntek's vice president, to become closely involved in the DoD's budding information technology research.[153]

For Poindexter, Project Genoa's goal of enabling the Pentagon to take preemptive security measures was reminiscent of his experiences as White House military assistant, and later national security adviser, under the Reagan administration. Following John Hinckley Jr.'s failed 1981 assassination attempt on President Reagan, Poindexter developed an interest in "crisis preplanning" and established a White House "crisis preplanning group" that discussed the use of information technology to forecast security threats.[154] However, the group's discussions faded in importance as the nation's political machinery became embroiled in the controversies surrounding the Iran-Contra Affair and Poindexter's central role in the scandal was revealed.[155] Not long after, Poindexter was convicted of five felonies, including perjur-

Island Networks Will Participate in JWID—Premier Interagency and Military Interoperability Event (June 14, 2004), *available at* http://www.swanisland.net/news/releases/032904-01.html [hereinafter Press Release, Swan Island Networks].

148 Dawn Onley, *Barriers to Info Sharing Remain: Interview with Defense Department CIO John Grimes*, Government Computer News, Sept. 11, 2006, *available at* http://www.gcn.com/print/25_27/41900-1.html [hereinafter Onley].

149 *Ibid*.

150 Scott Berinato, *Poindexter Comes in from the Cold: The man behind the government's canceled antiterrorism Total Information Awareness program explains for the first time what went wrong and how, in fact, it may not really have been canceled after all*, CIO, Aug. 1, 2004, Vol. 17, No. 20 [hereinafter Berinato].

151 *Ibid*.

152 *Ibid*.

153 *Total Business Awareness: The Corporate Contracting Behind John Poindexter's Total Information Awareness Program*, Multinational Monitor, Jan. 1, 2003, at 21 [hereinafter *Total Business Awareness*].

154 Berinato, *supra* note 150.

155 George Edmonson, *Poindexter's new Caldron: Senators Suspect Admiral in Terrorism Wager Plan*, The Atlanta Journal-Constitution, July 31, 2003, at 15A [hereinafter Edmonson].

ing to Congress.[156] Though his convictions were later overturned on grounds that prosecutors had violated Poindexter's right against self-incrimination,[157] his political career appeared to have come to a close.

In January 2002, however, after Poindexter had collaborated with DARPA for five years as the vice president of Syntek, the Pentagon hired him to direct its information technology research.[158] By this time, Project Genoa had evolved into a program called Total Information Awareness (TIA), a multi-dimensional data-mining project that embraced Poindexter's strategy of managing terrorist threats preemptively.[159]

The primary objective of TIA was to develop the technological capability to track terrorists' preparations for planned attacks. Software designed as part of the TIA program would enable computers to search a high volume of commercial transactions for activities that, while alone may seem innocent, together form a pattern suggesting an individual is involved in planning acts of terrorism.[160] Information yielded from the searches would be shared with appropriate intelligence and law enforcement officials so that potential terrorists could be identified and intercepted before the threat of attack became imminent. As Poindexter explained, "If terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions, and they will leave signatures in this information space."[161] By searching for series of transactions that signal terrorist activity rather than investigating individuals to determine if they match a "terrorist profile," TIA had the potential to spotlight suspicious activities of individuals not yet known to intelligence agencies.

An operational TIA would have required the development of technologies facilitating large-scale government surveillance of international commercial transactions. Airline ticket purchases, hotel reservations, and medical records, as well as information about credit cards, passports, driver's licenses, and gun purchases[162] were some of the transactions TIA sought to monitor in order to decipher patterns of suspicious behavior. Some reports indicated that information gathered from transaction searches would be by surveillance obtained from highly sophisticated cameras installed in public areas.[163]

In addition to data mining, TIA also involved initiatives to improve information sharing. One attempt to encourage policy experts to share their insights was a developing program known as FutureMAP. The goal of FutureMAP was to establish an electronic futures market in which experts could wager on hypothetical political and economic events.[164] The possibility of winning a wager would provide an incentive for policy and terrorism experts to participate actively and offer accurate predictions. At the same time, information gathered on the experts' collective predictions would be valuable to policymakers in assessing the likelihood that particular events would or would not occur.[165] Poindexter urged that innovative measures for collecting information would significantly enhance the nation's security against terrorist threats. He insisted, "We must become much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options."[166]

156 *Ibid.*
157 *Ibid.*
158 *Total Business Awareness, supra* note 153.
159 Berinato, *supra* note 150.
160 William New, *The Poindexter Plan*, The National Journal, Sept. 7, 2002, Vol. 34, No. 36.
161 *Ibid.*
162 Michael J Sniffen, *Pentagon's Terrorism Research Lives on at Other Agencies*, USA Today, Feb. 22, 2004, *available at* http://www.usatoday.com/tech/news/techpolicy/2004-02-22-tia-lives-on_x.htm [hereinafter Sniffen, *Pentagon's Terrorism Research*].
163 Daniel Weintraub, *Too Much Information: Feds Can't Get Enough of It*, Sacramento Bee, Nov. 19, 2002, at B7.
164 Berinato, *supra* note 150.
165 *Ibid.*
166 *Ibid.*

Understanding the Failure of Total Information Awareness

Congress's awareness of the FutureMAP program instigated the unraveling of most TIA initiatives and led to the rapid dissolution of Poindexter's office. Though TIA and its predecessor, Project Genoa, had received some $42 million in funding over a five-year period[167] and would have received $8 million more by 2007,[168] members of Congress of both parties were dismayed by the civil liberties implications of Poindexter's information technology initiatives.[169] In particular, FutureMAP was not viewed as an innovative sharing tool, but rather as a disturbing gambling proposal. California Senator Barbara Boxer opined that there was "something very sick about" the program.[170] When the website of an independent contractor involved in the project listed the assassination of Yasser Arafat and the overthrow of Jordan's King Abdullah II as examples of events on which wagers could be placed on FutureMAP, Democratic Senator Ron Wyden of Oregon criticized the program as "a federal betting parlor on atrocities and terrorism."[171] Poindexter insisted that such futures would not have been permitted on FutureMAP and that the program had been gravely misunderstood. He claimed that the information appearing on the contractor's website had offered "extremely bad examples [of the FutureMAP program] that had not been approved"[172] by the DoD. Nevertheless, Congress deemed the program "unbelievably stupid" and decided to shut it down within twenty-four hours.

Poindexter's data mining strategies likewise received an unfavorable reception from Congress. Several vocal Republicans considered the strategy "absurd," with then Senate minority leader Tom Daschle denouncing TIA as "perhaps the most irresponsible, outrageous, and poorly thought-out of anything that I have heard the administration propose to date."[173] Over Poindexter's objections, his technology program was renamed "Terrorism Information Awareness."[174] Though the DoD maintained that all legal restrictions on the collection and use of personally identifiable information would guide TIA programs, public relations initiatives were not sufficient to quell virulent reactions to Poindexter's programs. Public interest and civil liberties advocates lamented the difficulty of preventing and detecting abuse of data mining technology and argued that Poindexter's programs blurred the boundaries between the national security agencies of the military, intelligence, and law enforcement communities.[175]

At the same time, editorialists and members of the public criticized TIA as a massive operation for spying and collecting data records on law-abiding Americans without warrants or probable cause.[176] Represented by a logo containing the pyramid and eye that appear on the back of a dollar bill and the motto, "Knowledge is power," TIA was condemned by the media as an alarming government effort to create an "Orwellian 'Big Brother' society."[177] In response to Poindexter's controversial

167 Berinato, *supra* note 150.

168 Jim Mannion, *Poindexter to Resign: Defense Official*, Agence France Presse, July 31, 2003 [hereinafter Mannion].

169 *Ibid*.

170 George Edmonson, *Poindexter to Quit Job at Pentagon*, The Atlanta Journal-Constitution, Aug. 1, 2003.

171 Michael J Sniffen, *Poindexter Says He Hopes Congress Will Save Part of his Terrorism Research*, Associated Press, Aug. 14, 2003 [hereinafter Sniffen, *Poindexter Says He Hopes*].

172 *Ibid*.

173 Berinato, *supra* note 150.

174 Ted Bunker, *Capital Focus: DARPA, Like It or Not, Must Push Envelope,* The Boston Herald, Aug. 4, 2003, at 27.

175 John Markoff, *Poindexter's Still a Technocrat, Still a Lightning Rod*, N.Y. Times, Jan. 20, 2003, *available at* http://query.nytimes.com/gst/fullpage.html?sec=technology&res=9A07E4DF1530F933A15752C0A9659C8B63 [hereinafter Markoff].

176 Siobhan Gorman, *Adm. Poindexter's Total Awareness*, Nat'l Journal, May 8, 2004, Vol. 36, No. 19 [hereinafter Gorman].

177 Bob Keefe, *Poindexter: Domestic Monitoring Program May Come Back*, Cox News Service, Apr. 20, 2004.

programs, websites belonging to Cryptome, San Francisco Weekly, and several private individuals began to collect and list information about Poindexter, including his address, telephone numbers, email address, and home photos.[178] Stephen DeVoy, a computer scientist who created a website called the "John Poindexter Awareness Office" in November 2002, argued that such forms of Internet protest were designed to "mak[e] him [Poindexter] feel watched in the same way other people would feel watched"[179] by TIA programs.

Amid the controversy, the DoD affirmed that technologies being developed by Poindexter's office were not the basis of a domestic spying system and that their use would be guided by legitimate policies to protect the nation against terrorist strikes. In late 2002, Rumsfeld suggested that the public outcry had severely misrepresented TIA's programs, commenting, "The hype and alarm approach is a disservice to the public."[180] Poindexter defended his research programs by explaining that data-mining technologies were not to be used to amass government data records on private individuals but rather to aid human intelligence analysis capabilities by identifying patterns of suspicious behavior.[181] He claimed his office was aware that it would not receive "an uncontrolled flow of information"[182] and stated that privacy and civil liberties policies would necessarily limit the use of new technologies. He also emphasized the importance of continued funding for TIA research and reminded policymakers that his office was also responsible for several non-controversial programs for improving information sharing and foreign language translation.[183] Nevertheless, Congress discontinued funding for TIA in September 2003, several weeks after Poindexter resigned from office.[184] Poindexter would later explain that anxiety over TIA reflected a deficit of public awareness about terrorism and national security policy, which he referred to as a "failure of public diplomacy."[185]

Despite Congress's unwillingness to openly consider the merits of Poindexter's research, it permitted the transfer of some of his projects, estimated at a cost of approximately $64 million,[186] to classified, or "black,"[187] elements of the defense budget that defy public awareness. Congress's decision offered a rapid response to public outcry but in the long-term, deepened the anxieties of civil liberties advocates and citizens concerned about privacy. Unlike TIA, the classified programs are no longer subject to public monitoring and lack the degree of transparency necessary to prevent the abuse or misuse of information. Requiring that the DoD conduct information technology in secret also prevents the Department from fostering public confidence in new security strategies. Steve Aftergood of the Federation of American Scientists has referred to Congress's decision as a "shell game" and suggested that the classified DoD programs may be conducting research indistinguishable from Poindexter's TIA, minus public scrutiny.[188]

The collapse of TIA was arguably triggered as much by controversy surrounding Poindexter's political history as by ill reception to his unorthodox technological proposals. When the goals of TIA clashed with civil liberties agendas, memories of Poindexter's involvement in the Iran-Contra Af-

178 William Reitz, *Poindexter's Past Haunts TIA Program*, California Policy St. Univ., Feb. 28, 2003.
179 Puzzanghera, *Turning Tables on Government: Web Site Posting Data on Database Monitor,* San Jose Mercury News, Dec. 19, 2002.
180 Derrick Z Jackson, *Who's Watching the Watchers?,* Boston Globe, Nov. 22, 2002, at A25.
181 Markoff, *supra* note 175.
182 Berinato, *supra* note 150.
183 Sniffen, *Poindexter Says He Hopes, supra* note 171.
184 Michael J. Sniffen, *Poindexter Resigns, Says His Terrorism Research Was Misunderstood*, Associated Press, Aug. 13, 2003.
185 Gorman, *supra* note 176.
186 Sniffen, *Pentagon's Terrorism Research, supra* note 162.
187 Hiawatha Bray, *A Wasted Opportunity in War on Terror*, Boston Globe, Aug. 15, 2005, at E2.
188 Sniffen, *Pentagon's Terrorism Research, supra* note 162.

fair contributed to a sense of mistrust regarding the expansion of information technology research. Though Poindexter graduated first in his class at the Naval Academy in 1958, possesses a doctorate in nuclear physics, and is credited with having superior computer expertise,[189] he is criticized as "politically tone-deaf."[190] Dr. John Prados, a military historian at the National Security Archive, summarized perceptions of Poindexter with his claim that "From the beginning Poindexter has been a technocrat involved with the manipulation of information."[191]

An expert on electronic records at the of University of Michigan's School of Information named David A. Wallace argued that Poindexter's past indicated a propensity to use technical expertise to circumvent safeguards on civil liberties. "When faced with a system of checks and balances [during the Reagan administration], he [Poindexter] decided to act illegally. What does this say about the person who we are putting in charge of designing the most comprehensive surveillance system on U.S. citizens ever?,"[192] Wallace asserted when controversy over TIA flared in January 2003. Wallace, as well as other critics of Poindexter's character, however, failed to carefully consider the purpose of the TIA program. Poindexter's technology would have enabled the government to conduct high-powered searches to discover patterns within vast amounts of data but was not designed to support massive databases warehousing private information about American citizens. In his resignation letter, Poindexter expressed his "regret that we have not been able to…reassure the public that we do not intend to spy on them."[193]

Democratic Senator Byron L. Dorgan of North Dakota, who was vocal in denouncing TIA, has insisted, "The issue wasn't Poindexter. The issue was preposterous ideas that in some cases threatened the privacy of the American people."[194] However, both Poindexter and Rumsfeld have acknowledged that Poindexter's controversial past made it difficult for the DoD to engage in an informed dialogue with Congress and the public concerning TIA.[195] One indication that the debate over TIA had been clouded by judgments of Poindexter's political past was that similar DoD technology research projects had been led by John Hamre, President Clinton's Deputy Secretary of Defense, with little controversy. Hamre did experience difficulties in his work, though his problems stemmed not from public opposition but rather from the technical complexity of developing pattern-detecting technology. In fact, Hamre acknowledged that under Poindexter's direction, the DoD had made significant strides in resolving technical challenges as well as developing privacy safeguards that he considered "much stronger than the privacy protection we have now" for the handling of personally identifiable information.[196] Former Deputy Attorney General and 9/11 Commissioner Jamie Gorelick concurred, admitting that "If it [TIA] hadn't been at the Pentagon, if it hadn't been John Poindexter, it might have gotten a different reception."[197]

Before Congress had even considered drafting a legal framework to support an information sharing environment, Poindexter recognized the integral role of information collection, analysis, and sharing in managing terrorist threats to U.S. national security. In his view, privacy safeguards would necessarily regulate technological capabilities developed by TIA. However, he considered it more appropriate that elected officials, rather than DARPA's technical specialists, determine the balance between security needs and civil liberties protection demanded by the Constitution. At a mini-

189 Edmonson, *supra* note 155.
190 Markoff, *supra* note 175.
191 *Ibid*.
192 *Ibid*.
193 Sniffin, *Poindexter Says He Hopes, supra* note 171.
194 Carl Hulse & Thom Shanker, *Senators Want to Block Spending on Terrorist Initiatives*, N.Y. Times, Aug.14, 2003, at 20.
195 Mannion, *supra* note 168.
196 Gorman, *supra* note 176.
197 *Ibid*.

mum, continued funding of Poindexter's research would have provided policymakers with a greater variety of security tools, which likely would have aided current interagency information sharing initiatives. Though Poindexter has never officially stated that TIA could have prevented September 11th, the 9/11 Commission identified an inability to "connect the dots" as a primary government failure leading up to the terrorist attacks. TIA would have provided analysts with many more "dots" and assisted them in deciding which were important and how they should be connected.

DoD Collaboration with the Intelligence Community

At the time when TIA faced imminent collapse, the DoD was also working on other initiatives to enhance horizontal data sharing and replace "stovepipe" mentalities with information policies better suited to support modern missions. By July 2003, the Defense Information Systems Agency (DISA) in Arlington, Virginia had broadened civilian agencies' access to terrorism information by integrating eighteen federal agencies into the Pentagon's Defense Switched Network (DSN).[198] Lt. Gen. Harry Raduege Jr., DISA's director, also led projects to increase the availability of DoD bandwidth for the improvement of communications in anti-terrorism operations.[199]

Since the enactment of the IRTPA, the DoD has taken steps to implement the ISE by advancing its relationship with the Intelligence Community (IC) and developing a more comprehensive strategy for information sharing. DoD CIO John Grimes has stated that he is "aggressively collaborating"[200] with the IC through frequent meetings with retired Air Force Major General Dale Meyerrose, who has served as CIO of the Office of the Director of National Intelligence (ODNI) since August 2005. General Richard B. Myers, former Chairman of the Joint Chiefs of Staff, told Congress in 2005 that increased collaboration between defense and intelligence officials will enable the DoD to "incorporat[e] Intelligence Campaign plans into Operational plans" and better "inform the intelligence community of what the war-fighters need."[201]

In their conferences, CIOs Grimes and Meyerrose have concentrated on fostering trust between the DoD and the ODNI and building upon technical improvements in defense and intelligence information sharing that have occurred over the last 18 months.[202] In March 2006, the DoD and ODNI established the Unified Cross Domain Management Office to oversee the merger of hundreds of information systems, holding data of various classification levels, into approximately twenty basic cross domain solutions (CDS).[203] The primary mission of the Office, which is headquartered in Adelphi, Maryland, is to facilitate the movement of classified information across secure federal networks.[204] Meyerrose has described the creation of the Unified Cross Domain Management Office as "the first of many combined endeavors" that the ODNI and DoD will initiate to fuse defense and intelligence information capabilities "into closer alignment as we move to a more integrated, collaborative enterprise."[205]

The operations of the Unified Cross Domain Management Office are facilitated by the Certification and Accreditation (C&A) Transformation, a

198 John Rhea, *DoD Information Network Expands to Support Anti-Terrorism Activities*, Military & Aerospace Electronics, July 1, 2003, No. 7, Vol. 14.

199 *Ibid*.

200 Wilson P. Dizard III, DOD, *Spy Agencies Expand Sharing Plans: Project Aims to Cross Classification Levels*, Government Computer News, Mar. 19, 2007, Vol. 26, No. 6 [hereinafter Dizard].

201 *Fiscal 2006 Appropriations: Defense*, CQ Congressional Testimony, Apr. 27, 2005 [hereinafter *Fiscal 2006 Appropriations*].

202 Dizard, *supra* note 200.

203 *Ibid*.

204 *DoD CIO and DNI CIO Establish New Office to Enhance Information Sharing Between DoD and the Intelligence Community*, Pub. Interest Services, Mar. 8, 2007.

205 Dizard, *supra* note 200.

joint DoD and IC initiative seeking to standardize procedures governing access to information. By ensuring that certifications and accreditations apply across intelligence and defense agencies, the Transformation will simplify security controls and avoid duplicative "re-accreditation" procedures.[206] After eight-months of collaboration with the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), Commonwealth Partners, as well as independent contractors and academia, Grimes and Meyerrose have developed common goals to guide the reform of C&A procedures.[207] Their objectives, announced in March 2007, include diminishing the numbers of IC Protection Levels and DoD Mission Assurance Categories (MAC) by creating common "trust levels."[208] Coordination of security control procedures will be further supplemented by the formation of joint risk management policies[209] that cultivate a culture of support and collaboration.

Integration of DoD and IC information handling procedures was advanced in July 2007, when Grimes and Meyerrose signed a memorandum of agreement setting forth a joint strategy for improving defense and intelligence interoperability. The strategy guides implementation of a services-based information environment that will be managed by a cooperative body co-chaired by the Grimes and Meyerrose.[210] By offering services, rather than "stand alone applications"[211] to support the DoD and IC's respective missions, the strategy adopts a commercial approach to improving data flow through the use of Web-based technology. The agreement and "services oriented" strategy are likely to serve as a sharing model for other federal ISE participants.

DoD Information Sharing Strategy and Net Centric Operations

Continued collaboration between the defense and intelligence communities has shaped the DoD strategy for implementation of the ISE, which was released in May 2007. The DoD Information Sharing Strategy, which sets forth a vision for sharing with federal, SLT, foreign, and private sector partners, was created by the Office of the Secretary of Defense and the Joint Chiefs of Staff through close collaboration with ISE program manager Ambassador Ted McNamara. The DoD Strategy provides objectives and values that will guide the incremental processes of creating a "transparent, open, agile, and…trusted" information environment.[212]

The strategy is largely the result of the Pentagon Office of Transformation's (OFT's) numerous studies analyzing the role of information sharing in military missions and defense actions requiring interagency cooperation, such as the response to Hurricane Katrina.[213] These studies highlighted concrete benefits of information exchange and explored ways to increase sharing. The studies also emphasized that past efforts to improve defense communications have consisted primarily of investments in technology rather than organizational or structural changes.[214] According to John Gartska, assistant director of concept and operations at the OFT, the studies exposed the need to eliminate

206 *DNI & DoD Chief Information Officers Announce Certification and Accreditation Transformation Goals*, PR Newswire-US Newswire, Mar. 27, 2007, *available at* http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/03-27-2007/0004554328&EDATE=.
207 *Ibid*.
208 *Ibid*.
209 *Ibid*.
210 Press Release, Department of Defense, DoD and DNI Chief Information Officers Establish Shared Vision for a Joint Services Based Environment to Enable Information Sharing,(July 19, 2007), *available at* http://www.defenselink.mil/releases/release.aspx?releaseid=11146.
211 *Ibid*.
212 Press Release, Department of Defense, New DoD Strategy Outlined for Information Sharing, (May 4, 2007), *available at* http://www.defenselink.mil/releases/release.aspx?releaseid=10831.
213 Michael Sirak, *DoD Expands Studies of Combat to Understand Networked Forces*, C4I News, Feb. 2, 2006.
214 *Ibid*.

the "chasm" between information sharing technology and policy, a military need he considers "just as important as stealth."[215]

Among the DoD's goals to improve information sharing, the DoD Information Sharing Strategy prioritizes four aims for achieving greater integration of information capabilities. First, the DoD will intensify efforts to shift from a "need to know" culture to a "need to share" environment by providing incentives for sharing and ensuring that DoD leaders promote this key cultural change.[216] Second, the DoD will "achieve an extended enterprise," which includes all participants of a mission, that functions with greater coordination and agility.[217] Third, the DoD will expand capabilities to manage unexpected events and sharing partners, "proactively plan for information sharing," and preempt potential challenges.[218] Finally, the DoD will concentrate on building trust with its sharing partners.[219]

Though the DoD Information Sharing Strategy is only a twenty-four-page document addressing information sharing in broad terms, a more detailed, comprehensive plan for guiding the DoD's role in implementing the ISE is expected in October or November of 2007. This supplementary report will address governance, resources, technology, and infrastructure issues involved in the information sharing policy transformation, as well as the culture, organization, and philosophies that are critical to its success.[220]

The DoD approach to information sharing is informed by the Pentagon's decision to modify military strategies to accommodate Net Centric operations, a goal embodied in the DoD's *Joint Vision 2020*.[221] The concept of Net Centric Warfare (NCW) combines battlefield strategy with Information Age technology to augment military capabilities for coordinated decision-making. Engaging in NCW involves "networking" forces, on "all levels of command and control down to the individual soldier," to receive real-time battlefield information and achieve synchronized situational awareness.[222] U.S. forces are striving to move toward networking. However, NCW as described in *Joint Vision 2020* will require an expensive transformation and technological capabilities that are currently in the research and development phase.[223]

The key to success as a networked force is improved information sharing among the DoD's internal forces and organizations as well as its foreign allies. Kenneth Krieg, Under Secretary of Defense for Acquisition, Technology and Logistics, has emphasized that networks and information sharing "are the lifeblood of military and civil operations."[224] The DoD has therefore issued a Net-Centric Data Strategy that relies upon networks to enhance coordination, information management, and interoperability.[225] Because data net-centricity is "user-oriented,"[226] the Net-Centric Data Strategy encourages authorized participants to post information on DoD networks rapidly to ensure that it is available for users needing to pull data.[227] Thus, the Strategy avoids a "pre-formatted, tightly

215 *Ibid*.
216 Dept. of Defense, DoD Information Sharing Strategy (May 4, 2007), available at www.defenselink.mil/cio-nii/docs/Info**SharingStrategy**.pdf.
217 *Ibid*.
218 *Ibid*.
219 *Ibid*.
220 Daniel Friedman, *Strategy Set for Sharing Information*, Federal Times, May 14, 2007, at 9.
221 Gregory Belenky, et al, *Cognitive Readiness in Network-Centric Operations*, Parameters, Spring 2005.
222 *Ibid*.
223 Michael J Golden, *JNN—Network Selected as 2006 IDGA Network Centric Warfare Award Winner*, Army Communicator, Sept. 22, 2006, Vol. 31, No. 4.
224 *Defense Science Board Examines Military Implications of Google, Blogs*, Inside the Pentagon, Apr. 13, 2006, Vol. 22, No. 15 [hereinafter *Defense Science Board*].
225 Dept. of Defense, DoD Net-Centric Data Strategy (May 9, 2003), available at www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf.
226 Onley, *supra* note 148.
227 *Ibid*.

controlled approach" to data management by urging that users "post [information] before processing."[228] Though the Net Strategy was disseminated before he assumed his position as DoD CIO, John Grimes has advanced net-centricity by directing the U.S. Strategic Command (STRATCOM) and the Defense Information Systems Agency to establish a center for facilitating data sharing across DoD organizations.[229] In addition, the DoD is implementing a Global Information Grid that will serve as a framework for net-centric operations among U.S. forces and foreign allies. When fully operational, the system will coordinate collaborative decision-making, data management, and information services in a user-oriented "worldwide information network."[230]

According to a 2006 Navy study, information sharing and the early development of net-centric technologies have resulted in "dramatic improvements in performance," even where networking efforts remain "limited."[231] However, the DoD faces challenges in ensuring information security in a networked system and promoting a culture of sharing. David S. Alberts, research director in the Office of the Assistant Secretary of Defense for Networks and Information Integration, has lamented, "Some older officers don't want to get out of their comfort zone."[232] Overcoming hostile mindsets, he suggested, will involve efforts to clearly define the concepts driving NCW and the benefits of increased sharing.[233] Training, determined leadership, and incentive driven policies to share are factors that will play a key role in creating a more coordinated and integrated environment for defense information.

Multinational Information Sharing

The need for improved interoperability among U.S. forces and coalition partners in the Global War on Terror (GWOT) drives the DoD to develop processes and technologies to advance the establishment of an international information sharing environment. In addition to promoting net-centric operations through the creation of the Global Information Grid (GIG), the DoD established a Joint Program Office and multinational executive agent in 2005 to support the Pentagon's Multi-National Information Sharing (MNIS) efforts.[234]

The U.S. has recently coordinated sharing initiatives with NATO allies through a system known as Link 016[235] and through joint efforts to establish net-centricity. In addition, NATO, as well as, the national forces of "Australia, Canada, Finland, France, Germany, Sweden, Turkey, and the United Kingdom" have participated in information sharing tests and demonstrations with the U.S. military.[236] An organization known as the Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition (MAJIIC) Project Working Group, which consists of representatives of U.S. Joint Forces Command (USJFCOM) and NATO's Consultation, Command and Control Agency (NC3A), has advanced multinational sharing by hosting information exchange simulations and technology demonstrations.[237] These events have provided an opportunity for U.S. military personnel and NATO allies to test emerging technology, understand the

228 *Ibid*.
229 *STRATCOM, DISA Plan New Center to Improve DoD Information Sharing*, Inside the Pentagon, Dec. 7, 2006, Vol. 22, No. 49.
230 *Joint Staff Directorate Calls for Multinational Info Sharing Review*, Inside the Pentagon, Oct. 21, 2004, Vol. 20, No. 43.
231 *Study: Net-Centric Enhancements Yielded 'Dramatic' Results in OEF*, Inside the Pentagon, Mar. 15, 2007, Vol. 23, No. 11.
232 Peter Buxbaum, *DoD Prepares to Leap Net-Centricity Gaps: IT Security, Change Management Among the Most Prominent*, Gov't Computer News, Vol. 25, No. 24 [hereinafter Buxbaum].
233 *Ibid*.
234 *Fiscal 2006 Appropriations*, *supra* note 201.
235 Onley, *supra* note 148.
236 Buxaum, *supra* note 232.
237 *USJFCOM, Coalition Partners Seek MAJIIC Solution to Coalition ISR Interoperability*, News from USJFCOM, Feb. 10, 2006, available at http://www.jfcom.mil/newslink/storyarchive/2006/pa021006.htm.

challenges of information exchange, and hone data sharing techniques.

While information sharing efforts are expected to improve coordination with NATO forces, DoD CIO John Grimes has stressed that "[o]perations in Afghanistan and Iraq have highlighted the need to…incorporate unanticipated coalition members and partners."[238] For example, U.S. Air Force Gen. Paul V. Hester has explained that information exchange with allies in the Pacific presents difficulties as "the lack of a NATO-like structure" means "the United States must often deal with each nation independently."[239] The MNIS, according to Grimes, is thus designed provide a "standardized means for sharing information with ad hoc coalitions."[240]

On a regional level, the DoD has conducted simulation exercises between U.S. Southern Command (SOUTHCOM) and South American forces, including the Argentine Military and the Honduran Permanent Committee on Contingencies (COPECO) in order test the effectiveness of emerging information technology in crisis situations.[241] In Africa, U.S. European Command (USEUCOM), along with representatives of Austria, Sweden, and Norway, has hosted a program called Africa Endeavor (AE) to integrate U.S. military information capabilities with those of over twenty African nations.[242] While AE will likely assist a range of military operations, including humanitarian and disaster responses, U.S. Air Force Brigadier General Thomas Verbeck has urged that the information sharing program "will help USEUCOM achieve its goals [in the] war on terrorism, regional security and transformation."[243]

In addition to engaging in multilateral efforts to improve sharing, the DoD has also cooperated with individual nations. Since 2006, the U.S. and Japan have explored networking mechanisms that will facilitate the sharing of missile defense data collected by each nation's respective radars.[244] The two nations also reached a general security of military information agreement (GSOMIA) in May 2007 to promote the sharing of defense and intelligence information.[245] Similarly, the U.S. and Canada have shared intelligence information on the North American maritime environment that will allow each nation to achieve "comprehensive, combined" awareness of vulnerabilities and security threats.[246] United States Northern Command (USNORTHCOM), the North American Aerospace Defense Command (NORAD), and Canada Command have additionally collaborated in training exercises designed to identify effective information sharing processes for responses to homeland security threats.[247]

Supporting Technology

The DoD's strategic and organizational efforts to improve information sharing have been supplemented by IT development and innovative uses of existing technology. Many initiatives to im-

238 Onley, *supra* note 148.

239 *Passing the Efficiency Test With Flexible, Deployable Comm*, Air Force Communications Agency, June 1, 2007, http://public.afca.af.mil/news/story.asp?id=123055539.

240 Onley, *supra* note 148.

241 *USSOUTHCOM Conducts Multinational Crisis Management Experiment*, United States Army News, Dec. 14, 2006, available at http://www.army.mil/-news/2006/12/14/977-ussouthcom-conducts-multi-national-crisis-management-experiment/.

242 *Multinational Workshop to Integrate Communications Systems Among African Militaries*, European Command Pub. Affairs, July 6, 2006, http://www.eucom.mil/english/FullStory.asp?art=1044.

243 *Ibid.*

244 Takashi Imai Yomiuri Shimbun, *Japan, U.S. to Boost Antiballistic Info Sharing*, The Daily Yomiuri, Jan. 15, 2006.

245 3rd *LD: Japan, U.S. Press N. Korea on Denuke Step, Allies Expand Data Sharing,* Japan Policy & Politics, May 7, 2007.

246 *U.S., Canada Developing Shared Maritime Intelligence Picture*, Inside the Pentagon, Nov. 20, 2003, Vol. 19, No. 47.

247 *DND: Canada Command Exercises in Support of Civil Authorities*, Canadian Corporate Newswire, Apr. 11, 2007.

prove data collection, analysis, and sharing have been prompted by the need to assist war fighters in Afghanistan and Iraq in maintaining situational awareness and some have already had their effectiveness tested on the battlefield.

One effort to expand technical capabilities has centered on information sharing software in development at Swan Island Networks, Inc., a five-year old Portland, Oregon company that specializes in enabling organizations to share sensitive information across secure networks.[248] In 2004, U.S. Northern Command (NORTHCOM) featured Swan Island Networks' software in the Joint Warrior Interoperability Demonstration (JWID), an esteemed annual event that evaluates emerging command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) technologies.[249] Of particular interest to the DoD is Swan Island Networks' SWARM technology, which facilitates the sharing of sensitive homeland security data by maintaining information security across federal, state, and local networks.[250] In addition to providing a secure system to connect organizations, SWARM can support NORTHCOM's coordination of homeland defense missions by transmitting alerts, enabling exchanges, and targeting users.[251]

Emerging technology is also critical in supporting military operations abroad. U.S. Joint Forces Command (USJFCOM) has effectively relied upon the WebFile Server (WFS) developed by Xythos Software. The WFS enhances coordination and information sharing within the Cross Domain Collaborative Information Environment (CDCIE) that currently links U.S. and Coalition Forces in Iraq.[252] The Web-based system provides a secure environment for document management and exchange by multiple users.[253] The WFS also offers a "scalable collaboration application,"[254] as it was specifically designed to support larger collaborative environments such as the CDCIE. In addition to its use of Xythos Software, the DoD enhances communication among coalition partners through the Combined Enterprise Regional Information Exchange System (CENTRIX), which links thousands of users representing more than sixty countries in order to improve the coordination of operations in Iraq.[255] Army Brig. Gen. Jeffrey W. Foley has commented that use of CENTRIX is a key step toward moving from a "need to know" to a "need to share" culture between the U.S. and its foreign allies.[256] According to Foley, the support provided by CENTRIX is "one of the most monumental success stories in the history of joint and coalition war fighting."[257]

While integrating innovative software into the collaborative environments of its domestic and overseas operations, the DoD is also leveraging existing technology to meet emerging needs. Instant messaging, typically thought of as a civilian recreational technology, has proven a useful tool for expanding communications across the Army, Navy, Air Force, and Marines.[258] The distinguishing feature of military instant messaging technology, much of which has been provided by the Washington company Bantu, Inc., is that the communications remain secure.[259]

In Iraq, where web-based technology like Xythos software, as well as CENTRIX, e-mail, and vid-

248 Press Release, Swan Island Networks, *supra* note 147.
249 *Ibid*.
250 *Ibid*.
251 *Ibid*.
252 *U.S. Joint Forces Command Deploys Xythos to Support Multinational Forces in Iraq*, Business Wire, Mar. 29, 2005.
253 *Ibid*.
254 *Ibid*.
255 *Information Access Key in Terror War, CENTCOM General Says*, American Forces Press Service, Mar. 31, 2005, http://www.defenselink.mil/news/newsarticle.aspx?id=31057 [hereinafter *Information Access Key*].
256 *Ibid*.
257 *Ibid*.
258 Deborah Funk, *Military Services to Enlist Instant Messaging Network*, Federal Times, Apr. 10, 2006, at 8 [hereinafter Funk].
259 *Ibid*.

eo teleconferencing have all been integrated into military communications, secure chat rooms are also being established to allow rapid exchanges of information. Army Brig. Gen. Foley has stated that chat rooms, which simultaneously coordinate the instant messages of multiple users into a single conversation, have facilitated numerous military activities, including the dissemination of information gathered from patrols and the tracking and striking of "lucrative target[s]."[260] One of the greatest assets of instant communication technology, he explained, is that they "effectively coordinate the time-sensitive targeting process."[261]

The need for greater sharing of terrorism and homeland security information has provided an impetus for creating a consolidated DoD instant messaging network that allows military personnel to target and communicate with users of disparate branches of the service. Since Bantu, Inc. has provided similar software to the Departments of Commerce, State, and Homeland Security, some government users predict that the ease and speed of instant communications systems will encourage the development of interagency instant messaging capabilities.[262] Kenneth Krieg, Under Secretary of Defense for Acquisition, Technology and Logistics, has also stated that search engine technologies supporting "googling" and "blogging" activities "are making their way into military operations at all levels."[263] However, he added that the use of such technologies is experimental. "The full implications of this revolution are as yet unknown and we have no clear direction and defined doctrine,"[264] he claimed.

While expanding its communication networks, the DoD has remained cognizant of the need for data security and continues to stress the risks of cyber threats. In 2007, the DoD decided to devote $2.5 billion to projects on "information assurance," which include the research and development of biometric identification systems.[265] Currently, the DoD relies upon firewalls and technology referred to as "software patches"[266] to prevent unauthorized access to data. However, DoD CIO John Grimes has recently stated that the frequency of Internet and e-mail attacks on defense data by hackers has increased dramatically.[267] He claims that the department is "under attack 24 hours a day."[268] Grimes explained, "If you can't protect information, you can't share it."[269] Thus, as ISE implementation makes information sharing an increasing priority, the DoD may be expected to intensify its efforts to develop expanded security capabilities and sophisticated access controls.

Assessing Remaining Challenges

The DoD has launched numerous information sharing initiatives and is producing technology that will more effectively coordinate sharing with both internal and external partners. However, the Department still faces cultural hurdles and obstacles to developing trust. Overcoming these challenges will be necessary if the DoD is to successfully promote a "need to share" environment.

Though the DoD Information Strategy and the implementation plan due later this year should assist cultural transformation, available evidence indicates the need for the DoD to clarify, in practical terms, how information sharing should affect daily operations. In addition, the DoD must close gaps between emerging technology and personnel training. Marine Corps Maj. Gen. Michael Ennis has explained that in some cases, "The people in the field don't have a clue that the [relevant] web site even exists, much less the ability to go find

260 *Information Access Key, supra* note 255.
261 *Ibid*.
262 Funk, *supra* note 258.
263 *Defense Science Board*, *supra* note 224.
264 *Ibid*.
265 *DoD Intertwines Data Security, Interoperability Challenges*, Government Computer News, Mar. 19, 2007, Vol. 26. No. 6.
266 Onley, *supra* noe 148.
267 *Ibid*.
268 *Ibid*.
269 *Ibid*.

it."[270] Striking a balance between advancing information sharing through technology research and implementing organizational strategies should therefore remain a priority. Technology alone will not be sufficient to deconstruct the "stovepipe systems" that DoD CIO John Grimes claims still impedes information sharing efforts.[271]

The DoD information sharing processes have also been criticized as inadequate in the context of homeland security. In 2004, a report by a Defense Science Board task force urged that the Pentagon "fundamentally rethink"[272] homeland security information sharing and clarify its role vis-à-vis civilian agencies in this area. Critics have also pointed out that the DoD should intensify efforts to exchange information on critical infrastructure vulnerabilities to bolster the preparedness of NORTHCOM.[273]

Homeland Security

The Department of Homeland Security (DHS) has played an integral role in pioneering efforts to increase vertical information sharing between federal and state, local, and tribal (SLT) ISE participants. DHS has developed an increasingly successful partnership with state and local intelligence fusion centers, enabling federal authorities to more carefully integrate fine-grained information about domestic terror threats into their understanding of the nation's security landscape. The Department has also endeavored to create a large-scale network to support federal and SLT communications on homeland security issues. The network, however, has encountered great difficulty in meeting the needs of its users and must be urgently improved if a fully operational ISE is to be implemented by 2009.

"Fusing" Federal, State, and Local Terrorism Information

In response to its observation that a lack of vertical communications had severely hampered the nation's ability to connect evidence of the 9/11 plot, the 9/11 Commission promoted the concept of state and local information fusion centers.[274] These information centers are designed to synthesize, analyze, and share federal, state, and local information on homeland security issues. Since September 11, 2001, fusion centers have been established in forty-two states and the District of Columbia. In December 2005, President George W. Bush directed that these states and local institutions be integrated into the ISE, an effort that is largely coordinated by the Department of Homeland Security's (DHS) State and Local Fusion Center Implementation Plan (SLFC Plan).[275]

By gathering, investigating, and sharing available local evidence, each fusion center contributes to the mosaic-like effort of forming a coherent picture of national homeland security threats. PM-ISE Ted McNamara has referred to the work of fusion centers as a "critical part of the information sharing capability" and U.S. antiterrorism efforts. He has also emphasized that as federal and SLT entities "work[] towards an era of increasing collaboration" through implementation of the ISE, fusion centers are likely to emerge as examples of how strategic partnerships can result in tangible accomplishments.[276] Similarly, Charles E. Allen, the DHS' CIO, has referred to fusion centers as a "center of gravity"[277] for information sharing across multiple levels of government.

270 Jean, *supra* note 144.
271 Onley, *supra* note 148.
272 *DoD Urged to 'Fundamentally Rethink' Homeland Security Info Sharing*, Inside the Pentagon, Oct. 14, 2004, Vol. 20, No. 42.
273 *Ibid*.
274 Shane Harris, *Fusion Centers Raise a Fuss*, The Nat'l Journal, Feb. 10, 2007 [hereinafter Harris].
275 *Ibid*.
276 *Officials Hold First Ever National Fusion Center*, PR Newswire-US Newswire, Mar. 8, 2007 [hereinafter *Officials Hold Fist Ever National Fusion Center*].
277 *Information Sharing*, CQ Congressional Testimony, Sept. 7, 2006 [hereinafter *Information Sharing*].

Existing fusion centers differ greatly across states and localities in both size and the nature of their operations. Though some fusion centers concentrate on information sharing with federal entities, such as DHS and the Federal Bureau of Investigation (FBI), many others focus on enhancing local investigations of suspicious activity.[278] States and localities have also devoted varying amounts of resources to their fusion centers. Therefore, some rely primarily upon human analysis while others have incorporated sophisticated software and data-mining technology into their daily operations.[279]

Most centers, however, collect their information from a variety of sources and seek to synthesize data gathered from public informants, the media, and local investigations.[280] A fusion center in Phoenix, Arizona for example, has made regular use of a myriad of sources, including "police reports…names, addresses, contact information, business cards, [and] tickets"[281] in its attempt to analyze local homeland security threats. Other fusion centers have reported using both "public and commercial databases" and "data discovery" software, such as the Factual Analysis Criminal Threat (FACTS) program provided by LexisNexis.[282]

While enhancing security through information analysis, fusion centers also amass a body of "actionable intelligence"[283] for local law enforcement authorities and first responders. A fusion center called the Maryland Coordination and Analysis Center, which is located outside Baltimore, runs a twenty-four-hour "watch section" that tracks informants' tips and real-time evidence of suspicious activity. [284] Lt. Robert Fox, the co-program manager of a Los Angeles intelligence fusion center, claims that fusion centers make it possible to "do what everyone calls 'connecting the dots,'"[285] the intelligence analysis effort that the 9/11 Commission had concluded was weak and uncoordinated in the period leading up to the September 11th attacks.

Despite fusion centers' varied approaches to analyzing intelligence information, the integration of fusion centers into the ISE requires some degree of uniformity across jurisdictions. The SLFC Plan, which was approved by Secretary Michael Chertoff on June 7, 2006, offers a framework for coordinating both horizontal information sharing across fusion centers as well as vertical sharing between fusion centers, state and local governments, and federal authorities. The Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 both provide statutory authority for DHS' development of the SLFC Plan. To allow for continuity of operations and efficient integration of fusion centers into the ISE, DHS has relied heavily upon the President's Information Sharing Guidelines in developing the policies outlined by the Plan.[286]

According to DHS CIO Charles Allen, the goal of the SLFC plan is to "ensure that state and local officials are tied into the Department's [of Homeland Security] day-to-day operations" and that DHS officials are "embedded" in the daily work of fusion centers.[287] The federal strategy for real-

278 Mary Beth Sheridan, & Spencer S. Hsu, *Localities Operate Intelligence Centers to Pool Terror Data; 'Fusion' Facilities Raise Privacy Worries as Wide Range of Information is Collected*, Wash. Post, Dec. 31, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/30/AR2006123000238.html [hereinafter Sheridan].

279 *Ibid*.

280 Harris, *supra* note 274.

281 Sheridan, *supra* note 278.

282 Alice Lipowicz, *Data Mining Gets a Makeover: Call It Fusion as New Tools Expand Hunt for Terrorists*, Wash. Technology, Sept. 18, 2006 [hereinafter Lipowicz].

283 *State and Local Information Sharing*, CQ Congressional Testimony, Mar. 14, 2007 [hereinafter *State and Local Information Sharing*].

284 Sheridan, *supra* note 278.

285 Lipowicz, *supra* note 282.

286 *Homeland Security Information Network*, CQ Congressional Testimony, Sept. 13, 2006 [hereinafter *Homeland Security Information Network*].

287 *Fiscal 2008 Budget: DHS Office of Intelligence and Analysis*, CQ Congressional Testimony, Feb. 14, 2007 [hereinafter *Fiscal 2008 Budget*].

izing this strategic partnership involves supplementing fusion center staffs with DHS personnel, who will assist local officials in collecting and analyzing homeland security information. DHS representatives will also facilitate the sharing of fusion center information with federal intelligence, homeland security, and law enforcement authorities. On the federal level, Allen, who considers the integration effort "one of the Department's most important initiatives,"[288] coordinates and oversees the federal/state networking process. Currently, DHS officials have been stationed in twelve fusion centers across the country, including locations in Georgia, California, Louisiana, Maryland, and New York.[289]

By providing personnel support to fusion centers across the country, the SLFC Plan embraces the notion that "one size does not fit all."[290] Instead, the Plan seeks to tailor federal efforts to the needs of specific fusion centers. DHS' commitment to meeting the needs of individual fusion centers is reflected by its initiative to conduct detailed assessments of fusion centers' information strategies, technological and analytic capabilities, data security, and mission concentrations. Upon completion of each study, DHS devises a set of recommendations on integrating the particular fusion center into the ISE. DHS also collaborates with the FBI, the Department of Justice (DOJ), the National Counter-Terrorism Center, and intelligence agencies to ensure that homeland security, law enforcement, and intelligence information gathered by fusion centers are all adequately and effectively shared in the ISE.[291] This collaborative effort enables the federal government to "speak[] with 'one voice' to state and local partners."[292] By September 2006, DHS had conducted assessments of twelve fusion centers, including those located in Columbus, Ohio; Phoenix, Arizona; North Central Texas; Albany, NY; Richmond, VA; Springfield, IL; Tallahassee, FL; San Diego, CA; Los Angeles, CA; San Francisco, CA; and Sacramento, CA.[293] In addition to DHS' willingness to review the needs of individual fusion centers, the Department has provided considerable policy and technical support, as well as funding totaling over $380 million, in the period between 2001 and 2006.[294]

DHS' leadership recognizes that successfully integrating fusion centers into the ISE will require a considerable amount of time and careful work. The SLFC Plan therefore sets forth a timetable that permits integration to occur at a gradual and manageable pace.[295] The Plan has received praise for avoiding the temptation of setting unrealistic goals. In a September 7, 2006 hearing of the House Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Allen stated, "I want to promise only what we can deliver and expect only that which each center can provide to us."[296]

According to McNamara, integration of fusion centers into the ISE will allow the centers to remain directed by state and local entities while also guiding them to perform "primarily analytical" functions that aid national counter-terrorism and homeland security initiatives.[297] McNamara envisions the development of a genuine partnership between federal and fusion center analysts and continues to emphasize the importance of two-way vertical information sharing. Just as local law enforcement officials require federal cooperation to effectively protect their jurisdictions from terrorist activity, federal authorities are increasingly relying upon information gathered and analyzed

288 *Homeland Security Information Network, supra* note 286.
289 *Assessment of Information Sharing Centers*, CQ Congressional Testimony, Sept. 7, 2006 [hereinafter *Assessment of Information Sharing Centers*].
290 *Ibid*.
291 *Homeland Security Information Network, supra* note 286.
292 *Ibid*.
293 *Information Sharing, supra* note 277.
294 Sheridan, *supra* note 278.
295 *Assessment of Information Sharing Centers, supra* note 289.
296 *Ibid*.
297 Sheridan, *supra* note 278.

by local officials in order to detect homegrown terror plots.[298]

In the long-term, DHS hopes to fulfill the President's goal of establishing a National Network of Fusion Centers.[299] Secretary Michael Chertoff explained to the Senate Committee on Homeland Security and Government Affairs on September 12, 2006, that such a Network would create a system wherein federal "intelligence and operations personnel [would be] at every state and major metropolitan fusion center in the United States, sitting in the same room, sharing and analyzing information and intelligence in real time."[300] In March 2007, the Office of the Director of National Intelligence (ODNI), the DOJ, DHS, the FBI, and the Office of the Program Manager for the Information Sharing Environment advanced the President's goal by hosting over 580 attendees at the first annual National Fusion Center Conference.[301] The purpose of the conference was to discuss the potential establishment of a National Fusion Center and other mechanisms for coordinating federal analysis and use of information provided by state and local fusion centers.[302] Secretary Michael Chertoff affirms that realizing a National Network of Fusion Centers is a priority for his Department. "Working together—leveraging our networks, moving relevant information and intelligence quickly, and enabling rapid analytic and operational judgments,"[303] he maintains, will be a critical asset to the nation's security that DHS is working vigorously to implement.

Challenges of Vertical Information Sharing

While the federal government has experienced early successes in improving vertical sharing, efforts to increase federal collaboration with fusion centers have illustrated the challenges of sharing across multiple levels of government in a federalist system. Varying state law on the operation of fusion centers has compounded the difficulty of promoting some measure of uniformity across state and local homeland security initiatives.[304] Additionally, in a study conducted by the National Governors Association, sixty-percent of state homeland security directors claimed they were "unhappy about the specificity of intelligence" provided by federal partners.[305] These complaints suggest that the federal government has not effectively consolidated efforts to conduct vertical information sharing and that DHS' collaboration with the IC, the FBI, and the Office of the Program Manager should be strengthened.

State and local fusion center officials claim that they receive "mixed and at times competing messages"[306] from federal authorities, whose attempt to increase sharing has sometimes suffered from a lack of effective quality controls. In some cases, information from federal authorities duplicates what is already known by fusion centers or has not been updated by the time it is received by state officials.[307] One example of these difficulties surfaced publicly in October 2005, when New York City Mayor Bloomberg, informed by local fusion authorities, announced that "a specific threat" implicated the city's mass transit system.[308] Federal officials had already concluded that the threat was "noncredible,"[309] though timely communication between federal and state authorities analyzing the issue did not occur.

In other cases, state and local officials have struggled to receive urgently needed sensitive or classified information because they must wait lengthy

298 *Assessment of Information Sharing, supra* note 289.
299 *Fiscal 2008 Budget, supra* note 287.
300 *State and Local Information Sharing, supra* note 283.
301 *Officials Hold First Ever National Fusion Center, supra* note 276.
302 *Ibid*.
303 *Fiscal 2008 Budget, supra* note 287.
304 Harris, *supra* note 274.
305 Sheridan, *supra* note 278.
306 *Ibid*.
307 *Assessment of Information Sharing Centers, supra* note 289.
308 Sheridan, *supra* note 278.
309 *Ibid*.

periods for security clearances. In September 2006, Col. Kenneth Bouche of the Illinois State Police briefed the House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk on the difficulties imposed on fusion centers by federal security clearance procedures.[310] He called the classification system "archaic"[311] and "cumbersome"[312] and lamented that, contrary to the goals of the ISE, the system is "designed to keep information secret." DHS claims that it recognizes the difficulties pointed out by Bouche and is actively working to hasten background checks.[313] However, rapid improvement is unlikely, as federal agencies have only just begun the process of establishing uniform accreditation policies. Under the current system, a fusion center official who obtains an accelerated clearance from DHS will often still be unable to receive information classified at the same level from other agencies.

In response to testimony from state and local officials, Rep. Bennie Thomspon of Mississippi concluded that federal authorities are simply "not reaching out well enough"[314] to the state and local officials that need to be integrated into the ISE. While officials from DHS and the Office of the PM for the ISE continue to stress that fusion centers possess highly valuable information and play an integral role in ensuring the nation's security, the difficulties of seamlessly sharing real-time information on a vertical level mean that sometimes, fusion centers have been treated as "junior partners in the war on terrorism."[315] For example, Louis Quijas, assistant director of the office of state and local coordination at the FBI, has complained that years after Congress called for establishment of the ISE, he must often repeat to FBI officials that sharing with state and local partners at fusion centers should occur on a daily basis.[316]

Efforts to increase vertical sharing by pushing data "up" from fusion centers to the federal government have also experienced difficulties. While state officials display enthusiasm for increased collaboration with federal officials, they claim that they are often unsure which officials or agencies they should contact when they seek to share specific terrorism, homeland security, or law enforcement information. Moreover, the information they do provide is not always useful for federal purposes or arrives out of context. Continued difficulties on both sides of the sharing equation have prompted some authorities to predict that seamless sharing and full integration of fusion centers into the ISE may take as many as ten or more years to achieve.[317]

The Future of Fusion

Federal authorities must not be discouraged by the challenges of integrating fusion centers into the ISE. Despite difficulties, state officials claim that they can point to specific incidents in which increased collaboration has enhanced security.[318] Similarly, DHS officials have affirmed that efforts to pool federal, state, and local information analysis efforts by integrating fusion centers into the ISE have already strengthened U.S. counterterrorism capabilities.[319]

Improvements are likely to result from DHS' recently adopted, "aggressive schedule"[320] to station thirty-five more federal officials at fusion centers by the end of 2008. DHS is currently working with federal and state authorities to "determine which centers have the greatest need"[321] for immediate federal cooperation. However, DHS should also heed calls from state officials to develop a "clear-

310 *Assessment of Information Sharing Centers, supra* note 289.
311 *Ibid.*
312 *Ibid.*
313 *Ibid.*
314 Sheridan, *supra* note 278.
315 Magnuson, *supra* note 77.
316 *Ibid.*
317 *Ibid.*
318 *Assessment of Information Sharing, supra* note 289.
319 *Ibid.*
320 *Homeland Security Information Network, supra* note 286.
321 *Fiscal 2008 Budget, supra* note 287.

er road map"[322] for coordinating the flow of information to and from fusion centers. As the number homegrown terror threats, such as those experienced by the United Kingdom over the last three years, continues to increase, effective federal cooperation with state and local fusion centers will be necessary to identify and disrupt them.[323]

State and local fusion centers are likely to require enhanced federal assistance to fulfill their missions as participants in the ISE and DHS must be prepared to meet fusion centers' needs over the long haul. As local operations improve, federal agencies will benefit from the integration of information gathered by more than 800,000 local law enforcement officers into the ISE.[324] While much work remains to be accomplished, DHS' cooperation with fusion centers represents one of the federal government's most significant efforts to foster the robust vertical information sharing envisioned by the ISE Implementation Plan.

Homeland Security Information Network (HSIN)

The Department of Homeland Security's second major initiative to facilitate ISE implementation is the Homeland Security Information Network (HSIN). HSIN provides a national network for homeland security alerts, information, and response coordination to federal, SLT, and private sector ISE participants. HSIN is also a medium for reaching public health officials, transportation security officials, state homeland security advisors, governors' offices, and the National Guard, to whom DHS owes the responsibility of providing routine notifications and "threat-based risk assessments."[325] DHS has intended HSIN to serve as the primary sharing environment for sensitive but unclassified homeland security information. Since its rapid assembly in 2004, the HSIN has linked locations across all fifty States, as well as fifty-three major cities and five U.S. territories, to DHS' Homeland Security Operations Center (HSOC), which watches real-time homeland security threat information and coordinates domestic incident management.[326]

HSIN evolved from a pilot program originally sponsored by the Defense Intelligence Agency (DIA) known as the Joint Regional Information Exchange System (JRIES). JRIES had been launched in December 2002, to facilitate communication between the California Anti-Terrorism Information Center, the New York Police Department, and the DIA. After JRIES had assisted users in sharing information rapidly during the northeast blackout of summer 2003, management of the sharing initiative was offered to DHS, which had a larger budget for maintaining and expanding the system.[327]

Though the JRIES communications network was originally supported by Groove software, DHS transferred the system to secure web-based portals that allow for instant messaging and the development of document archives. In September 2006, Frank W. Deffer, Assistant Inspector General for Information Technology at DHS, told the House Homeland Security Subcommittee of Intelligence, Information Sharing and Terrorism Risk Assessment that HSIN was also supplemented with a series of other information sharing features, including "suspicious incident and preincident information, mapping and imagery tools, 24/7 situational awareness, and analysis of terrorist threats, tactics, and weapons." The design of HSIN applications is intended to provide a platform for real-time communications and nearly comprehensive homeland security resources.[328]

322 Wilson P. Dizard III, *States Rap DHS Info-Sharing*, Gov't Computer News, Sept. 8, 2006, http://www.gcn.com/online/vol1_no1/41924-1.html.
323 *Fiscal 2008 Budget, supra* note 287.
324 *Assessment of Information Sharing Centers, supra* note 289.
325 *Homeland Security Information Network, supra* note 286.
326 *Ibid.*
327 *Ibid.*
328 *Ibid.*

HSIN also hosts two pilot sharing projects known as HSIN-Intel and HSIN-Secret (HSIN-S). HSIN-Intel was created to augment the flow of sensitive but unclassified (SBU) data, unclassified intelligence, and state and local law enforcement information through the HSIN network.[329] In 2006, intelligence officers, fusion center analysts, and senior law enforcement executives from the states of Arizona, California, Florida, Illinois, New York, and Virginia were linked to the experimental system.[330] Since then, documents exchanged on HSIN-Intel have included both "finished" intelligence information, which has been processed and analyzed, as well as "raw" information that may be of immediate assistance to various participants.[331] The design of the HSIN-S program is very similar to the HSIN-Intel network. HSIN-S, however, provides access to information classified at the secret level, and only carries a minimal amount of unclassified data.[332]

Evaluations of the pilot programs HSIN-Intel and HSIN-S, separate from the general functioning of the broader HSIN network, indicate a fair amount of success. In addition to accelerating the speed with which information flows between federal, SLT, foreign, and private sector actors, HSIN-Intel's sharing tools have enabled federal authorities to better synthesize information from fusion centers with DHS and IC data.[333] In a September 2006 congressional hearing, DHS CIO Charles Allen reported that HSIN-Intel participants have made active use of the experimental network, resulting in over five hundred document posts within the first five months of the pilot.[334] He also noted that the system greatly aided domestic and international communications following the July 11, 2006 transit bombings in Mumbai, India.[335] On that day, DHS "transmitted relevant intelligence reporting, held a 'quick-look' teleconference…and was able to provide valuable information that was not already widely available to the public" all through HSIN-Intel.[336] DHS is currently seeking to expand HSIN-Intel and prepare the network to become fully operational.[337]

Because of the difficulties of sharing classified information, particularly across multiple levels of government, HSIN-S has seen fewer posts and less frequent use from connected authorities.[338] Therefore, DHS has decided to integrate HSIN-S into "a more robust Secret-level classified communications network system" called the Homeland Security Data Network (HSDN) that is expected to enhance sharing opportunities for public and private sector personnel already possessing a Secret level clearance.[339] HSDN is currently being installed at state and local fusion centers.[340]

While DHS should build upon the successes HSIN-Intel and work to expand HSIN-S, it is imperative that the Department devotes sufficient resources to improving the primary information platform, HSIN. As further discussed below, HSIN has experienced difficulties to such considerable extent that there is a risk DHS officials may recoil from HSIN's problems to focus on the more successful, unclassified and secret networks. However, HSIN offers connectivity to a wider array of participants for broader horizontal and vertical sharing than does either of the pilot programs. Moreover, many private sector actors essential to the nation's effort to protect critical infrastructure are not linked to HSIN-Intel and lack necessary security clear-

329 *Ibid.*
330 *Assessment of Information Sharing Centers, supra* note 289.
331 *Homeland Secuirty Information Network, supra* note 286.
332 *Ibid.*
333 *Ibid.*
334 *Ibid.*
335 *Assessment of Information Sharing Centers, supra* note 289.
336 *Ibid.*
337 *Ibid.*
338 *Homeland Security Information Network, supra* note 286.
339 *Ibid.*
340 *Ibid.*

ances to participate in an expanding HSIN-S network.[341]

Problems Abound

Nearly all assessments of HSIN indicate that the system has failed to perform its intended function of serving as the principal nationwide network for homeland security information sharing. Since DHS took control of the JRIES program and launched HSIN, state and local law enforcement officials and fusion center analysts, HSIN's primary users, have claimed that the system does not aid them in accomplishing their missions.[342] DHS must redouble efforts to improve HSIN and enable users to view the system in light of its capabilities rather than its previous failures. So long as state and local officials turn to other sharing mechanisms, the nation faces the risk that an effective, consolidated network for exchanging terrorism and homeland security information on a nationwide scale will not be implemented.

Though DHS intended HSIN to provide an outlet for seamless and nearly comprehensive vertical information sharing, many current users are unfamiliar with the network's purpose and design.[343] They find that the system fails to meaningfully supplement state information sharing policies and tools, as much of the classified and situational awareness information they need is not available on HSIN.[344] Moreover, state and local officials have expressed reservations about information security on HSIN.[345] In September 2006, Frank W. Deffer, Assistant Inspector General for Information Technology at DHS, claimed that an "erosion in trust"[346] has occurred between law enforcement officials and DHS since management of JRIES had been transferred from DIA. DHS CIO Charles Allen has similarly concluded that state and local users "are not fully committed to the HSIN approach."[347]

Numerous reports from the DHS Inspector General and the Government Accountability Office (GAO) agree with state and local assessments of HSIN's inadequacy. Evidence of the network's failure to effectively enhance information sharing is disheartening in light of one GAO report's estimation that DHS has been spending approximately $300 million per year to operate and maintain HSIN. David Powner, Director of Information Technology Management Issues at GAO summarized criticism of HSIN when he told Congress that the system "has been poorly managed and poorly coordinated" and that without considerable improvement, HSIN "will not be the key information sharing network it is intended to be."[348]

HSIN's failures are largely attributable to its hurried implementation. The September 11th attacks had prompted not only a sense of urgency in improving security measures but also created the perception that a hastily planned information sharing tool was preferable to the delay of executing a carefully designed network. As the 2004 presidential elections drew near and intelligence officials warned of several possibly imminent terror threats, DHS officials faced considerable pressure to install a nationwide information system.[349] Lacking the time to develop a detailed framework or overarching vision for guiding HSIN's development, DHS simply pursued a rigorous timetable for installing HSIN across domestic and international locations.[350]

Time constraints prevented DHS from sufficiently cooperating with state and local officials to en-

341 *DHS Web Portals See Scant Use by Law Enforcement*, Wash. Internet Daily, Sept. 14, 2006.
342 *Homeland Security Information Network, supra* note 286.
343 *Ibid.*
344 *Ibid.*
345 Stephen Losey, *IG Blasts Data-Sharing Network*, Federal Times, July 10, 2006 [hereinafter Losey].
346 *Homeland Security Information Network, supra* note 286.
347 *Ibid.*
348 *Ibid.*
349 Losey, *supra* note 345.
350 *Homeland Security Information Network, supra* note 286.

sure that HSIN would be synthesized with existing state sharing practices. Though the Office of Management and Budget (OMB) provided DHS with guidelines on vertical collaboration, DHS did not thoroughly assess the needs of SLT actors, particularly fusion centers and law enforcement officers.[351] Many difficulties cited by local HSIN's local users stem from the federal "top down"[352] approach that DHS relied upon while rapidly installing the system. According to Connecticut Representative Christopher Shays, "The story of HSIN is a story of the federal government trying to impose a one size fits all approach on states and locals."[353] Given certain conditions beyond the federal government's control, such as varying state law on privacy and the use of homeland security information, many DHS officials adopted the position that a "top down" approach facilitated installation of the network and that any HSIN inadequacies could be reformed while the network is already in use.[354]

However, state and local complaints testify to the difficulty of contending with HSIN's ad hoc implementation plan retrospectively. HSIN's current functioning continues to reflect its history as an initiative that lacked clear goals, an organized governance structure, performance metrics or an understanding of its users' missions. Admiral Roger Rufe, Director of DHS' Office of Operations Coordination, wrote in an April 2007 memorandum that HSIN has "grown without sufficient planning and program management" but "for better or worse, is tied to DHS missions and operations."[355]

The question that remains is, as California Representative Jane Harman commented, whether the "HSIN DHS relationship" is simply "some bad marriage that we're all supposed to accept?"[356]

DHS's inability to reconcile the needs of its users has resulted in a situation where HSIN is frequently ignored in the course of fusion center and local law enforcement operations.[357] Even as the federal government attempts to prioritize information sharing through implementation of the ISE, DHS CIO Charles Allen has admitted that DHS is "behind in information management" and claimed, "I'm not happy with it, and I know the Secretary [Michael Chertoff] isn't either."[358]

Users are continually dismayed that many of HSIN's resources are already available on law enforcement networks while the system has done little to improve their ability to obtain federal intelligence information, often classified, that they urgently need.[359] Though some officials have claimed that HSIN has facilitated their information sharing efforts, Rep. Christopher Shays acknowledged that existing evidence suggests that the system "simply gathers dust" in many states.[360] Because local officials have had trouble discerning the purpose and goals of the system and federal authorities have not sustained an effort to integrate HSIN with existing sharing practices, many users are increasingly turning to other mechanisms to transmit and receive needed information.[361]

In some cases, these alternative mechanisms, such as telephone calls to officials' personal contacts in various locations, are admittedly slower and less efficient than web portal technology.[362] During the

351 Government Accountability Office, *Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*, Apr. 16, 2007.
352 *Fiscal 2008 Budget, supra* note 287.
353 *Fixing the Homeland Security Information Network: Finding the Way Forward for Better Information Sharing*, CQ Congressional Testimony, May 10, 2007 [hereinafter *Fixing the Homeland Security Information Network*].
354 *Fiscal 2008 Budget, supra* note 287.
355 *Fixing the Homeland Security Information Network, supra* note 353.
356 *Ibid.*
357 Losey, *supra* note 345.
358 *Ibid.*
359 *Fixing the Homeland Security Information Network, supra* note 353.
360 *Ibid.*
361 *Homeland Security Information Network, supra* note 286.
362 *Ibid.*

2005 London bombings, for example, U.S. law enforcement and transportation security officials found that HSIN "was no more useful or timely than information available via public news services" and preferred to communicate with contacts connected to London authorities than to rely upon HSIN.[363]

Perhaps of greater concern than officials' reliance on personal contacts than coordinated sharing mechanisms are recent initiatives is the reaction of some agencies, such as the U.S. Secret Service, to develop its own web-based systems for "information sharing among…limited user group[s]."[364] While these efforts may enable officials to provide enhanced security in the short-term, they severely disrupt DHS's and the federal government's broader goal of creating a consolidated sharing environment. Grassroots initiatives catering to the needs of particular users have the potential to increase the difficulty of resolving HSIN's inadequacies and establishing the network as the nation's primary homeland security information sharing tool. Ironically, as IG Richard Skinner pointed out, DHS's failure to provide a network meeting the needs of its users creates the risk that the alternative sharing mechanisms being developed will "only perpetuate[] the ad hoc, stove piped information sharing environment that HSIN was intended to correct."[365]

Improving HSIN

Implementation of a successful ISE demands that DHS prioritize efforts to improve HSIN. While DHS lacks the authority to require state and local officials to increase their use of HSIN or directly influence local sharing practices, DHS has the responsibility to offer its state and local partners a more efficient, useful system for information exchange.

Improving the current system must begin with increased DHS collaboration with state and local officials, the factor that was notably absent from HSIN's implementation procedure. As DHS has conducted studies on the missions and needs of fusion centers, the Department must similarly undertake a serious effort to recognize the needs of HSIN's targeted users. While developing an understanding of why HSIN has proven unsatisfactory to its users, DHS must also clarify the goals and purpose of the network for local officials who have expressed confusion and frustration about HSIN's intended role in their current operations.[366]

To ensure that the improved system will be used effectively, DHS should allocate resources for training and, as recommended by the DHS Inspector General, for the creation of "stakeholder-specific standard operating procedures" and the publication of "user manuals."[367] By assisting users in developing strategies for combining HSIN with current sharing practices, DHS can also reduce the problems of information duplication.[368] To improve the system's content, DHS must heed state and local officials' calls for inclusion of a greater amount of situational awareness information. DHS efforts to expedite security clearance procedures for fusion center personnel and private sector officials will also greatly enable the Department to update HSIN with greatly needed classified information.

DHS has made some improvements to HSIN's technical capabilities, content, and governance structure. The recently established Homeland Security Information Network Advisory Committee, a body of fourteen members, promises to represent federal, state, and local needs, as well as the specific concerns of first responders and private sector actors, regarding HSIN.[369] DHS recently

363 *Ibid*.
364 *Ibid*.
365 Losey, *supra* note 345.
366 *Homeland Security Information Network, supra* note 286.
367 *Ibid*.
368 *Fixing the Homeland Security Information Network, supra* note 353.
369 *Homeland Security Information Network, supra*

hired an HSIN Program Manager and created the HSIN Joint Program Management Office to oversee cooperation with strategic partners and ensure that HSIN meets standards mandated by the ISE Implementation Plan and the IRTPA. [370]

Despite these developments, DHS has yet to articulate a set of clear guidelines defining its strategy to improve HSIN and periodically assess the network's performance. Recent improvements of HSIN's governance structure are only first steps toward resolving HSIN's difficulties and consolidating sharing efforts among federal, state, and local officials with homeland security responsibilities. Until DHS demonstrates an ability to clear those obstacles, the ISE may experience significant shortcomings in the sharing of homeland security information.

Intelligence Community

The U.S. intelligence community (IC) has launched a sustained drive to modernize its intelligence-sharing procedures to respond better to 21st-century threats. Despite some valiant efforts, the available evidence suggests this initiative remains incomplete and requires a significant redoubling of efforts to achieve enduring results.

Since September 2001, the intelligence community has endeavored to improve information sharing by expanding its use of Open Source Intelligence (OSINT). Open-source intelligence (OSINT) is defined by the Department of Defense as "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[371] Open-source intelligence is important today in fighting the War on Terror and protecting national security and shows "both great promise and great production" according to CIA director General Michael Hayden. He also notes that former Director of National Intelligence John Negroponte "has been pushing for the agency to boost its analysis of open source intelligence."[372]

The Intelligence Reform and Terrorism Prevention Act of 2004 advocated the need for more open-source intelligence. Section 1052 discusses open-source intelligence and calls for the Director of National Intelligence (DNI) to "establish an intelligence center for the purpose of coordinating the collection, analysis, production, and dissemination of open-source intelligence to elements of the intelligence community."[373] Furthermore, it states that "open-source intelligence is a valuable source that must be integrated into the intelligence cycle to ensure that United States policymakers are fully and completely informed."[374]

Recent initiatives have made U.S. OSINT capabilities more robust. Nevertheless, several problems continue to impede the optimal exploitation of OSINT. The most important of these barriers are cultural rather than technological. Many analysts continue to undervalue unclassified sources of information.

History of Open-Source Intelligence within the IC

The convention within the U.S. intelligence community has been to focus intelligence gathering on three major sources. First, Human Intelligence (HUMINT) refers to the use of human intelligence agents and the recruitment of foreign agents. Second, Signal Intelligence (SIGINT) is the use of various eavesdropping methods to gather information. Third, Imagery Intelligence (IMINT) is

note 286.

370 *Ibid*.

371 National Defense Authorization Act for fiscal Year 2006, H.R. 1815, 109th Cong. (2007) (enacted), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ163.109.

372 Martin Sieff, *Analysis: Hayden faces uphill fight at CIA*, UPI, May 8, 2006.

373 6 U.S.C. § 485 at § 1052, *supra* note 14.

374 *Ibid*.

intelligence gathered by taking photos taken from satellites, unmanned vehicles or other types of reconnaissance.[375]

The fourth major source of intelligence that has been relatively untapped in the past is the use of Open Source Intelligence. Open Source Intelligence is derived from the collection, processing, and analysis of publicly available and unclassified information. This information is collected from a huge number of sources such as newspapers, television, training manuals, atlases, and even T-shirt slogans or graffiti[376]. Perhaps the most important source of OSINT today is the Internet, where websites, forums, blogs and chat rooms are all treasure troves of open source information.

The first modern use of open-source intelligence by the intelligence community started in the 1930s when the Foreign Broadcast Intelligence Service (FBIS), later renamed the Foreign Broadcast Information System, was established to collect and translate foreign open source intelligence information. It served as the open-source arm of the Central Intelligence Agency (CIA). Its collection and translation efforts of open source intelligence continued into the Cold War where OSINT "constituted a major part of all intelligence on the Soviet Union, China, and other adversaries."[377]

In general, however, the U.S. intelligence community has considered secret information far more valuable than the readily available media outlets that could technically be monitored by anyone. During most of the Cold War, OSINT operations were given approximately 1% of the total intelligence funding. With the end of the Cold War, this number went down to about half a percent[378]. By 1996, the Aspin-Brown commission found that there was a serious lack in the U.S. capability and efforts to gather and monitor Open Source Intelligence. The recommendations of the Aspin-Brown Commission to put more effort into OSINT were not followed through by several successive Directors of National Intelligence[379].

A major shift in the perception of OSINT came in the wake of 9/11. Several former intelligence professionals argued that al-Qa'eda threats prior to the 9/11 attacks could be found in openly available sources such as interviews and newspaper articles that were largely disregarded because they were not classified or secret documents.[380] In the 2002 Joint Congressional Inquiry into the Terrorist Attacks of Sept. 11, 2001, Republican Senator Mike DeWine lamented that the intelligence community was "more inclined to use open-source material as a last resort, not as a primary source, no matter how compelling the information.[381]"

In a report on the Intelligence Authorization Act for Fiscal Year 2007, the House Permanent Select Committee on Intelligence (HPSCI), stated that "the Intelligence Community must embrace more fully unconventional and open sources of information. Many estimate that large percentages of information needs can be satisfied by open source materials, and the Committee believes that the growth of the Internet and mass media has dramatically altered the amount of information available through open and unconventional sources."[382]

---

375 Scott Shane, *Intelligence Gathering Moves Out Into the Open,* The International Herald Tribune, Nov. 14, 2005, at 5 [hereinafter Shane].

376 *Ibid.*

377 Stephen C. Mercado, *Sailing the Sea of OSINT in the Information Age*, Studies in Intelligence, Vol 48 No.3 (2004), *available at* https://www.cia.gov/csi/studies/vol48no3/article05.html#rfn1 [hereinafter Mercado].

378 Charlie Allen, *The Department of Homeland Security: Second Review* Oct 19, 2005.

379 *OSS CEO Challenges DNI to Intelligence Duel*, PR Newswire, Apr. 13, 2006.

380 *U.S. Ignores Open-Source Intel Warning*, UPI, July 29, 2005.

381 Mike DeWine, *Additional Comments: Joint Inquiry Staff Report,* Report of the Joint Inquiry into the Terrorist Attacks of Sept. 11, 2001, S. Rep. No. 107-351, at 611 (Dec. 18, 2002), available at http://a257.g.akamaitech.net/7/257/2422/24jul20031400/www.gpoaccess.gov/serialset/creports/pdf/fullreport.pdf.

382 Intelligence Authorization Act for Fiscal Year

Congress sees the importance of open source intelligence and says, "To ignore the value of such information is dangerous." Finally, the Committee emphasized that "it will take a dramatic change in cultural philosophy to trust and use open source materials that weren't collected or discovered by 'secret means.'"

The Open-Source Intelligence Center

The September 2001 terror attacks catalyzed a major effort within the U.S. intelligence community to use open-source information more effectively. Subsequent investigations concluded that U.S. analysts had overlooked evidence of the impending al-Qa'eda attack that had appeared in publicly available sources such as interviews and newspaper articles.

In its final report, issued in 2004, the 9/11 Commission advocated the creation of a new Open Source Intelligence Agency. Following this recommendation, section 1052 of the Intelligence Reform and Terrorism Prevention Act of 2004 called on the new Director of National Intelligence (DNI) to "establish an intelligence center for the purpose of coordinating the collection, analysis, production, and dissemination of open-source intelligence to elements of the intelligence community." The subsequent WMD Intelligence Commission made a more detailed recommendation to establish an OSINT agency within the CIA.

In November of 2005, the Director of National Intelligence, John Negroponte, acted on the numerous recommendations and announced the creation of the Open Source Center (OSC), which was placed under the management of the CIA. OSC has become the new main body for OSINT, taking the place of its predecessor FBIS. The OSC is charged with supplying Open Source Intelligence to the sixteen intelligence agencies, the U.S. Defense Department and the U.S. Department of Homeland Security. In addition, the OSC develops guidelines and standards to create effective ways of exploiting open source material. The center centrally purchases and filters necessary data and thus relieves the need and the cost for other agencies to procure expensive data sets separately. The OSC is also a hub for training a new generation of open source experts.

By the middle of 2006, the OSC monitored roughly 300 Jihadist web sites and in terms of more conventional media outlets, OSC tracked approximately 500 television stations and a vast number of newspapers and radio broadcasts.[383] The OSC technology covers the filtering of data, foreign language processing, multimedia delivery and production, and the means of sharing information and collaborating with other agencies.[384] During 2006, at least 30 of the Daily Briefs presented to President Bush were based on Open Source Intelligence.[385]

Data archived by OSC permits its analysts to "draw upon it in response to queries from all levels of government,"[386] including state and local law enforcement and defense and national security agencies. DHS, for example, has "developed a concept of operations for aggressive use of open sources (OSINT) that leverages current activities of the Department, other departments and agencies including the DNI Open Source Center, the private sector, and our state and local partners in order to improve analysis and, when applicable, to protect intelligence sources and methods."[387]

2007, H.R. 109-411 (2006), *available at* http://www.fas.org/irp/congress/2006_rpt/hrpt109-411.html.

383 Patience Wait, *Intelligence Units Mine the Benefits of Public Sources*, Gov't Computer News, Mar. 20, 2006.

384 *Ibid*.

385 *Intelligence: Lawmaker Calls for Center to Become Independent Agency*, Technology Daily PM, June 7, 2006, Vol. 10:9 [hereinafter *Intelligence: Lawmaker Calls for Center*].

386 *Open-source intelligence moving to the fore*, Gov't Computer News, Nov. 16, 2006, Vol. 1, No.1.

387 Statement, Charles E. Allen, Asst. Secretary for Intelligence & Analysis Chief Intelligence Officer, Dept. of Homeland Security, *Examining Chief Intelligence Officer*

Furthermore, Assistant Secretary Charles Allen stated that "DHS officers will handle open-source information as a normal part of their everyday routine."

At the Annual Threat Assessment Hearings on January 11, 2007, Director of National Intelligence, John Negroponte, called U.S. intelligence "the best in the world," stating that recent reforms within the intelligence community, such as the establishment of the OSC, have further improved the intelligence gathering capabilities.[388] At the hearings, CIA Director Michael Hayden told the Senate Select Intelligence Committee that the CIA has raised the status and visibility of the newly formed Open Source Center (OSC) inside the CIA and that they "recognize its unique and growing contributions to integrated collection and analysis."[389]

Changes with Technology

With advances in technology, open-source intelligence has greatly expanded. According to Stephen Mercado's article on open-source intelligence, "The revolution in information technology, commerce, and politics since the Cold War's end is only making open sources more accessible, ubiquitous, and valuable."[390] Besides the constantly changing technology, the issues important to policy makers and the IC are also changing. A 2006 Congressional Research Services report entitled "Intelligence Issues for Congress" noted that OSINT "is increasingly important given requirements for information about many regions and topics (instead of the former concentration on political and military issues affecting a few countries)."[391] The report also expresses the belief of some observers "that intelligence agencies should be more aggressive in using OSINT; some believe that the availability of OSINT may even reduce the need for certain collection efforts."[392]

Besides monitoring Internet sites, U.S. intelligence analysts have sought to use new Internet tools—especially wikis and blogs—to store and manage information in innovative ways on its secure internal communication networks. Managers hope that wikis and blogs will make it easier for analysts to collaborate on issues that other analysts, typically working on related issues at different offices, might also be examining.

Blogs and Intellipedia

The use of blogs and wikis on intelink, "'the spy agencies' secure internal computer network"[393] is creating a new way to analyze intelligence. The new "Intellipedia" provides employees with a wiki (a website that allows for collective authorship) of people, places, and issues that all cleared employees can access and edit. The thought behind wikis and blogs is that analysts can contribute information on an issue that other analysts, perhaps at other agencies, are trying to figure out. In the fall of 2005, the DNI's head analyst got together with the chief technology officer and members of the CIA to create a prototype of Intellipedia, "a wiki that any intelligence employee with classified clearance could read and contribute to."[394] The reason for incorporating this into the intelligence community is to garner more collaboration and allow greater access to information and sources. By the fall of 2006, Intellipedia had 3,600 users and over 28,000 pages of information. Around the same

Progress, CQ Congressional Testimony, May 24, 2006.

388 *Senator John D. Rockefeller Holds Hearing on the Annual Threat Assessment*, CQ Transcripts, Jan. 11, 2007.

389 *Ibid.*

390 Mercado, *supra* note 377.

391 Richard A. Best, Jr., *Intelligence Issues for Congress,* Congressional Research Service, CRS Report RL33539, July 12, 2006, *available at* http://www.fas.org/sgp/crs/intel/RL33539.pdf.

392 *Ibid.*

393 Clive Thompson, *Open-Source Spying*, N.Y. Times Magazine, Dec. 3, 2006, *available* at http://www.nytimes.com/2006/12/03/magazine/03intelligence.html?ei=5090&en=46027e63d79046ce&ex=1322802000&partner=rssuserland&emc=rss&pagewanted=print.

394 *Ibid.*

time, a project was underway to create a National Intelligence Estimate from the information found on Intellipedia.

Members of the U.S. intelligence community are also relying more on Internet blogs (a web page that serves as a publicly accessible personal journal). Analysts can now create their own blogs on classified networks to express their opinions and ask for assistance on projects and issues they are examining. Analysts hope that the use of blogs and Intellipedia will help prevent another 9/11 or other serious terrorist attacks.

Problems Remain

Efforts to extend Open Source Intelligence gathering are still in the early stages, and a culture of reluctance towards open information within the intelligence community may continue to plague the efforts that are being made. In December 2006, CIA Director Michael Hayden told a large assembly of agency employees that CIA management intended to give OSINT specialists equal standing with agents relying on covert sources of data, thereby perhaps unintentionally acknowledging that many U.S. intelligence analysts and collectors continue to view OSINT experts as less than equal partners.

The biggest challenge facing the new Open Source Center is being able to provide the intelligence community with the intelligence, training, standards and personnel that it needs.[395] One of the most fervent advocates for increased OSINT gathering, former clandestine officer Robert Steele, has argued that the new OSC is both under-funded and understaffed.[396]

Concerns arise about the ability of the OSC to exploit Internet-based information, especially potentially rich data available on the growing number of Jihadist web sites. In a time where terrorist groups often use the Internet for recruitment and planning, there is a strong need for the U.S. intelligence community to further extend the capability to tap into these sources. The intelligence community has only recently modified its procedures to make it easier to recruit native Arab speakers as analysts and grant them security clearances.

Critics also worry that the U.S. intelligence community continues to undervalue OSINT relative to classified information. In a report to accompany the Intelligence Authorization Act for Fiscal Year 2007, the House Permanent Select Committee on Intelligence urged the U.S. intelligence community to embrace open as well as unconventional information sources. The report cautioned that recent experience suggested "it will take a dramatic change in cultural philosophy to trust and use open source materials that weren't collected or discovered by 'secret means.'" Eliot A. Jardines, Assistant Deputy Director of National Intelligence for Open Source says that such cultural change within the CIA is the most important goal. "Our culture is one that values secrecy, and we need to move beyond the notion that the higher the classification the better the intelligence," argues Jardines.[397]

House Republican Rob Simmons is a strong proponent of increased OSINT gathering, but he disagrees with the placing of OSC within the CIA. Simmons calls the OSC the "ugly stepchild" of the CIA and argues that it needs to be placed outside of the scope of the CIA in order to make it more independent.[398] The OSC is well aware of this issue and it has ensured that at least 25% of the personnel trained in OSINT were recruited from outside the CIA [399] The reliance on new recruits from

395 Robert K Ackerman, *Intelligence Center Mines Open Sources*, SIGNAL Magazine, Mar. 2006.

396 *Lawmakers want DHS to Make Full Use of Open-Source Intelligence*, Inside the Pentagon, Vol, 22:12, Mar. 23, 2006.

397 Bill Gertz & Rowan Scarborough, *Untitled*, The Wash. Times, Apr. 21, 2006, at A05.

398 *Intelligence: Lawmaker Calls for Center, supra* note 385.

399 Patience Wait, *Open Source Intelligence Moving to the Fore*, Gov't Computer News, Vol. 1:1, Nov. 16, 2006.

outside the CIA may work to counter the reluctance within the intelligence community regarding the use of open source information. Outside recruitment is likely to bring in young intelligence professionals who may be more inclined to look to open sources for information and more used to the idea that the Internet can be the best source of finding information. In order to make OSINT truly incorporated as an equal to the conventional intelligence gathering methods, a cultural shift also needs to occur on the highest levels of the intelligence community. The best way for this to occur is to simply create continuing evidence that OSINT is on par with conventional all-source intelligence gathering.

Conclusion

Open Source Intelligence will be a primary tool in gathering intelligence on several threats to U.S. security, including terrorism and the spread of avian flu. The new OSINT capabilities are far more robust today than they were a couple of years ago and the amount of open source intelligence that reaches policy makers has increased significantly as a result of changes in the intelligence community. Eliot Jardines, assistant deputy director of national intelligence for open source said that "the amount of open source reporting that goes into the president's daily brief has gone up rather significantly."[400] Mr. Jardines adds that "[t]here has been a real interest at the highest levels of our government, and we've been able to consistently deliver products that are on par with the rest of the intelligence community."[401]

U.S. Intelligence Managers Fighting with Overclassification

Notwithstanding the IRTPA's requirements, the campaign to establish the ISE has been plagued by "overclassification" and "pseudoclassification," both presenting major barriers to effective information sharing. The Chief Intelligence Officer in the Department of Homeland Security, Charles Allen, recently acknowledged that his staff was encountering serious resistance to implementing the "responsibility to provide" model propounded by current Director of National Intelligence Mike McConnell. Most prominently, the revelation that the Office of Vice President Richard Cheney has refused to comply with an executive order requiring it to file an annual report on how it handles classified national security information has highlighted several complex issues in this area.[402]

Within the U.S. government, classified information falls into two main categories. Information can be classified by the authority of Executive Order 12598, as amended, as Top Secret, Secret, or Confidential. Information that does not meet the standards established by the executive order, but that an agency considers sufficiently sensitive to warrant restricted dissemination, is classified as Sensitive but Unclassified (SBU). Documents under these seals range from law enforcement testimony to critical infrastructure data. The Information Security Oversight Office (ISOO) within the National Archives and Records Administration monitors implementation of federal government classification policies.

Proponents of generally limiting classified information offer six main reasons for revising current restrictions. First, greater information sharing promotes a more informed citizenry. Second, it makes government policies and practices more transparent and accountable. Third, it facilitates congressional oversight of intelligence operations. Fourth, reduced classification promotes efficiency in government management by reducing unneeded security costs. Fifth, the government can concentrate resources on protecting the most important information. Finally, greater information sharing

400 Bill Gertz, *CIA mines 'rich' content from blogs*, Wash. Times, Apr. 19, 2006, *available at* http://www.washtimes.com/national/20060418-110124-3694r.htm.

401 *Ibid*.

402 Richard Weitz, *Executive Order Dispute Highlights Problems with U.S. Government Secrecy Policy*, World Politics Review, June 25, 2007, *available at* http://www.worldpoliticsreview.com/article.aspx?id=879#.

makes it easier for analysts to integrate data from different sources, to counter groups (such as occurred with Iraq's nonexistent WMD), and helps achieve superior situational awareness of potential threats.

Overclassification and Pseudoclassification

The problem of overclassification refers to the classification of information that should not have been classified in the first place or that was given a higher than necessary level of classification. The challenge of pseudoclassification refers to the improper or overuse of the SBU designation.

The main cause of overclassification within the U.S. intelligence community is the continued adherence to the "need to know" principle. The Soviet bloc's comprehensive intelligence collection efforts during the Cold War justified the use of compartmentalized and decentralized intelligence operations. Terrorist groups, however, primarily use open source material and on-site observations to plan operations rather then attempt to steal classified information. For this reason, it is generally more effective to encourage a more liberal exchange of information to allow analysts to "connect the dots" to identify and preempt terrorist threats. The U.S. needs to replace the "need to know" approach with a "need-to-share" principle.

One easy application of such an approach would involve the greater use of "tear-lines" to separate out data from the sources and the methods used to obtain it. The tear-line report system protects the sources and methods—essential for recruiting human agents and obtaining information from foreign intelligence services—while allowing interagency exploitation of potentially illuminating intelligence. Its greater use would also facilitate intelligence sharing with Congress as well as state and local authorities.

In addition, President Bush has mandated the standardization of procedures for designating, marking, and handling SBU information across the federal government, but this goal remains unrealized five years after the 9/11 attacks. A 2006 audit by the Government Accountability Office (GAO) of how federal agencies treat SBU information identified 56 different designations for SBU information among the 26 agencies it surveyed. For example, the Department of Energy may mark documents with SBU information as "Official Use Only (OUO)", or it may choose to use another one of its sixteen designations for SBU information. In contrast, the Department of Defense uses the designation "For Official Use Only (FOUO)," and the Department of Homeland Security employs the designation "Protected Critical Infrastructure Information (PCII)."

Only a few of these categories, which probably number over a hundred in total, have any basis in formal statute. Most were created by individual agencies employing their own criteria and policies, resulting in the uncoordinated growth of designations that restrict vaguely defined classes of information. Unlike with classified information, moreover, government agencies typically do not provide means by which public groups can challenge SBU classifications.

This lack of a government-wide comprehensive interoperable SBU designation classification system interferes with information sharing in two ways. Not only do different agencies classify different information using different labels, but they often classify different information under the same labels. Indeed, the 2006 GAO report Information Sharing stated that half of the agencies covered reported encountering challenges in sharing SBU info. The GAO also found that most agencies do not limit who or how many employees have authority to make designations, provide adequate training for employees making designation decisions, or undertake periodic reviews to verify the proper use of classified designations.

In recent congressional hearings, many speakers from diverse backgrounds testified that the federal

government had yet to overcome these problems. For example, ISOO Director William Leonard stated that the number of federal government classification decisions has approximately doubled since the September 2001 terrorist attacks. As a result, the cost of managing the U.S. information classification system has reached a record high. An ISOO audit last year also found that almost two-thirds of trained classifiers they reviewed made mistakes in determining the appropriate level of classification.

Leonard did not address the issue of SBU data since it fell outside the oversight authority of his office—or any other independent executive branch body. Instead, individual agencies can decide for themselves whether they are correctly designating and managing sensitive information, effective vitiating the ISE. The program manager responsible for its implementation, Thomas McNamara, anticipates needing at least five more years before achieving "minimally" satisfactory progress—a problematic timeline.

Responding to long-standing concerns about the procedures and amount of classification within the federal government, the House Subcommittee on Intelligence, Information Sharing, and Terrorist Risk Assessment held hearings on the risks posed by overclassification of information by government officials. Speakers from a variety of backgrounds testified on the issues surrounding government classification and how it affects crucial information-sharing between all levels of government.

Almost all those who gave testimony to the committee agreed that the present culture of classification is excessive and dangerous both to national security and the right of the public to have access to non-vital information relating to government activities. The current system often fails to properly designate what truly needs to be kept confidential as well as hindering the effective sharing of information between federal agencies and local authorities. These tensions over the levels of government classification have existed for decades during the Cold War, but were brought to the forefront by the attacks on September 11th.

The 9/11 Commission in their final report directly cited overclassification as a major impediment to effective intelligence sharing in preventing future terrorist attacks. Security requirements fostered agencies to needlessly classify information and hoard intelligence within their own departments rather then effectively share it with other agencies.[403] The Commission further found penalties rather than incentives for individuals who effectively share intelligence between departments.

The Classification System

Classification authority is stipulated by Executive Order 12958 originally created by President Clinton and later amended by President Bush in 2003. Under the order, classification can only be mandated by assigned officials or by non-specified individuals who can clearly establish a line linking decisions by mandated officials that would justify classifying information. This system is monitored by the Information Security Oversight Office (ISOO), operating out of the National Archives and Records Administration.

This system relies on the ability of officials to responsibly classify truly sensitive information and not broadly use their authority to keep documents secret. With the terrorist attacks of 9/11 and the invasions of Iraq and Afghanistan, the amount of information that could potentially be seen as sensitive has increased. This has strained the abilities of officials to gauge what should be considered secret. In response to these increased pressures, officials have been erring on the side of caution and labeling more documents as classified. The Director of the ISOO William Leonard testified to this large increase citing that, "Classification

403 National Commission on Terrorist Attacks, *supra* note 1 at 435.

has multiplied, reaching 14.2 million classification decisions in 2005, nearly double the number in 2001."[404]

ISOO conducts yearly audits of the classification process of the federal government, including the financial costs associated with it. Its staff in conjunction with 41 executive agencies, excluding the CIA, calculated that $7.7 billion was spent on all aspects classification procedures in fiscal year 2005.[405] This sum was up nearly 5.8 percent from the previous year and represented an all time high for classification costs. Most of these increases dealt with physical security for classified information, including new employees and infrastructure costs.

In its annual report on the overall effectiveness of the classification process, the ISOO found numerous shortcomings in 2005. Its review of selected documents extrapolated that almost 66 out of every 100 documents had some form of error. Most problematic were the 10.6% of documents that had no label to designate why the document was being classified.[406] Furthermore the audit found that agencies did not effectively train their staff to be able to recognize what information truly needed to be classified.

ISOO's ability to help maintain a balance between the needs of national security and public disclosure has been difficult. They have struggled with the Bush administration's embrace of much more secrecy with regards to government information then previous administrations. One of the most public signs of this policy was a recent scandal at the National Archives. Historians were puzzled and shocked when seemingly innocuous documents previously declassified were suddenly removed and reclassified by various government agencies.[407]

The ISOO was asked to review the documents and found from a sample size that none of them appeared pose any threat to national security. However, the ISOO has no power to force an agency to change course. ISOO can merely make suggestions to the administration and Congress. The President is the only one who has that authority and has seemed unwilling to do so.[408]

Sensitive but Unclassified Data

The growth of a separate entity broadly identified as sensitive but unclassified information (SBU) has alarmed many observers. These documents have not been given a formal classification under Executive order 12958 but are instead given a variety of security labels that restrict access to them. Documents under these seals range from law enforcement testimony to critical infrastructure data. Agencies do not have to make the same reports on these decisions as they would under the formal classification system, eliminating ISOO oversight.

Around 56 different sensitive but unclassified labels are applied by a broad spectrum of federal agencies, the majority of them used by agencies involved in homeland security.[409] Only a few of these categories have any basis in formal statute, most are the product of individual agency policies. The individualistic nature of these classifi-

404 William Leonard, *Testimony to House Sub-Committee on Intelligence, Information Sharing, and Terrorist Risk Assessment*, Congressional Quarterly, Mar. 22, 2007.

405 *Report on Cost Estimates For Security Classification Activities for 2005*, Information Security Oversight Office, 2006, *available at* http://www.archives.gov/isoo/reports/2005-cost-report.pdf.

406 *2005 Report of the Information Security Oversight Office*, Information Security Oversight Office, May 25, 2006, *available at* http://www.archives.gov/isoo/reports/2005-annual-report.pdf.

407 Scott Shane, *US Reclassifies Many Documents in Secret Review*, N.Y. Times, Feb. 21, 2006, *available at* http://www.nytimes.com/2006/02/21/politics/21reclassify.html?pagewanted=1&ei=5088&en=370552525a85278d&ex=1298178000.

408 *Ibid.*

409 *Federal Government Needs to Establish, supra* note 43.

cations has at times inhibited effectively sharing them amongst agencies, since no overarching system exists on what information can be given out and to whom.

One of the major problems associated with SBU designations is the broad number of federal employees who can restrict access to data. At the DHS, Defense department, and Department of Energy almost any employee can apply a SBU related label on documents or information.[410] Compounding the large number of potential classifiers is the lack of effective training to help employees identify what needs to be kept sensitive and when the label is unnecessary. The DOE and DOD were cited in one report for their lack of a required training program for employees so they can accurately apply sensitive labels on materials.[411]

Ms. Meredith Fuchs of the National Security Archive noted, "The absence of reporting mechanisms for sensitive but unclassified control markings makes any assessment of the extent to which a policy is being used difficult, if not impossible."[412] Trying to get a completely accurate report on the entirety of SBU usage remains difficult. The lack of ISOO like body to watchdog SBU procedures means individual agencies are left with the responsibility of ensuring that they mark the correct information as being sensitive.

Rep. Christopher Shays(R-CT) member of the House Committee on Government Reform was highly critical of SBU data saying, "Legally ambiguous markings, like sensitive but unclassified, sensitive homeland security information and for official use only, create new bureaucratic barriers to information sharing."[413] He and many others finds these non-standardized security labels have the potential to impede vital intelligence sharing due to lack of a clear and recognized system for managing the variety of different brands.

Effects on Information Sharing

The Cold War mentality of compartmentalized and decentralized intelligence operations has proven ineffective in the new strategic environment. With the current emphasis on counter-terrorism, the Cold War mindset with "their dual requirements of appropriate security clearance and 'need to know' designation inhibit[s] the free flow of information to and from today's diverse community of relevant federal, state, local, and private sector actors."[414]

Al-Qa'eda does not operate the same sort of wide-ranging and extensive network of spies and informants as the Soviet Union once did. It primarily uses open source material and on-site observations to plan its operations rather then attempting to steal classified information. This calls into question the necessity of agencies tightly holding sensitive information to the degree that it impedes other intelligence community members from accessing it.

Even though more effective information sharing was both a recommendation of the 9/11 Commission and made law by various homeland security bills, a comprehensive system is still not in place with regards to sharing classified data. The Intelligence Sharing Environment (ISE), a product

410 David Perera, *Unveiling Secrets,* Gov't Executive, May 15, 2006, *available at* http://www.govexec.com/features/0506-15/0506-15na2.htm.

411 *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could be Improved*, Government Accountability Office, Mar. 7, 2006, *available at* http://www.gao.gov/new.items/d06369.pdf

412 Meredith Fuchs, *Testimony to House Sub-Committee on Intelligence, Information Sharing, and Terrorist Risk Assessment*, Congressional Quarterly, Mar. 22, 2007.

413 Rep. Christopher Shay, *Opening Remarks to House Sub-Committee on National Security, Emerging Threats, and International Relations Regarding Psudeo-Classifiation*, U.S. Gov't Printing Office, Mar. 2, 2005, *available at* http://a257.g.akamaitech.net/7/257/2422/07jun20051200/www.access.gpo.gov/congress/house/pdf/109hrg/20922.pdf.

414 James B. Steinberg, Mary Graham, & Andrew Eggers, *Building Intelligence to Fight Terrorism*, Brookings Institute, Sept. 2003, *available at* http://www.brookings.edu/comm/policybriefs/pb125.htm.

of the Intelligence Reform Act, was created to streamline the sharing between agencies at all levels of government.

As part of its mandate, it is attempting to create a government-wide plan for sharing and standardizing SBU information.[415] Its program manager, Thomas McNamara bluntly said, "We got everyone to agree, back in December of last year, that in principle, we need to change the way the federal government handles SBU."[416] No information has been released to suggest that a final set of recommendations has been given to the President for review. Analysts have been skeptical about the success of the program with Mary DeRosa of the Center for Strategic and International Studies commenting, "The program manager has a huge job and not enough staff...It has a long way to go."[417]

One of the continuing outcomes of this problem has been the lackluster information sharing between federal officials and their state and local counterparts. The FBI in particular has been very hesitant to give out clearances to state or local officials that would allow them to access more sensitive information.[418] Officials at the state and municipal level constantly feed information up to DHS and FBI, but frequently receive little reciprocal information back.

Local law enforcement has been continually frustrated by the current situation. Michael Downing of the Los Angles Police Department's Counter-Terrorism/Criminal Intelligence Bureau noted his agency's problem that local FBI offices can classify information as Secret, but do not have the authority to do the opposite and declassify documents.[419] Since state and local authorities are the first responders and the initial line of defense against potential terrorist threats, the current relationship badly hinders their ability to effectively coordinate security programs.

The question remains if there is enough impetus to try and fully implement the ISE, improve the classification system, and standardize SBU procedures. To do so would require massive shifts in the bureaucratic mentalities in numerous federal agencies as well as the full backing of the President and Congress. Ambassador McNamara noted, "We've got another at least five years of work to do before I would even be minimally satisfied that they're sharing information the way they ought to."[420]

Law Enforcement

The law enforcement community's investigative functions have prepared many of its officials for the responsibilities of information sharing in a national security context. However, a lack of consistent information procedures across law enforcement community participants has hindered the sharing of terrorism information on a nationwide scale. Recent Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) initiatives seek to establish a strategic partnership between federal and SLT law enforcement officials and improve the community's ability to develop standardized information sharing procedures.

The U.S. federal system of governance currently separates the law enforcement community into more than 18,000 SLT jurisdictions.[421] This struc-

415 *ISE Implementation Plan, supra* note 24.

416 Shane Harris, *All Together Now*, Gov't Executive, Mar. 15, 2007, *available at* http://www.govexec.com/features/0307-15/0307-15adif.htm [hereinafter Harris].

417 Alice Lipowicz, *Drift Into Nothingness: Information Sharing Initiative Slowed By Questions of Mission, Complexity* at 20, Wash. Technology, Oct. 10, 2005, *available at* http://www.washingtontechnology.com/print/20_20/27160-1.html.

418 *Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened*, Government Accountability Office, Aug. 27, 2003, *available at* http://www.gao.gov/new.items/d03760.pdf.

419 Michael Downing, *Testimony to House Sub-Committee on Intelligence, Information Sharing, and Terrorist Risk Assessment*, Congressional Quarterly, Mar. 22, 2007.

420 Harris, *supra* note 416.

421 Mark A. Marshall, *Understanding the National*

ture divides power among self-regulated law enforcement entities and maximizes accountability to local citizens. However, it also presents numerous challenges in launching unified policy initiatives, such as the establishment of a coordinated information sharing environment. Like fusion centers, law enforcement agencies must contend with variations in state law on issues such as information security, freedom of information, and privacy when attempting to share information across jurisdictions. Information access and quality control are two additional areas where the policies developed by autonomous law enforcement agencies tend to differ widely.[422]

Compounding the difficulties of reconciling inconsistent policies and legal requirements are cultural barriers to information sharing. Perpetuated in part by "need to know" practices, hostilities toward sharing have deterred some law enforcement officials from working collaboratively to "connect the dots" in gathering and analyzing terrorism information.[423] According to the DOJ, the law enforcement community's "institutional mistrust" represents "one of the most intractable barriers to improving information sharing."[424]

Despite the challenges of coordinating information sharing practices across a multiplicity of jurisdictions, the law enforcement community offers a valuable resource for increasing national awareness of terror threats. Effectively integrating the law enforcement community into the ISE promises to provide information on suspicious activity gathered by more than 800,000 police officers across the nation.[425] Local police officers likely have the greatest access to information about radical Islamists inspired by Osama bin Laden but not formally linked to the al-Qa'eda network. Through their ability collect information related to homegrown terrorist cells, law enforcement officers play a critical role in the nation's effort to counter domestic radicalization and develop a more coherent picture of terror threats.

Department of Justice Provides Needed Guidance

Noting that the law enforcement community suffers from the lack of a national strategy to coordinate information policy, the DOJ has launched the Law Enforcement Information Sharing Program (LEISP). The endeavor is intended to guide data exchange policies among law enforcement officials and prepare them for developing trusted information sharing partnerships with the defense and intelligence communities. Similar to the ISE, the LEISP is not an information "system" but rather a policy approach that facilitates the development of "need to share" procedures and encourages regular cooperation among participants. By emphasizing relationship building, accountability policies, and unity of effort, the LEISP seeks to ensure that law enforcement officials incorporate sharing into their daily operations.

The LEISP, which contains a National Information Sharing Strategy (NISS),[426] provides a framework for integrating the DOJ, as well as state and local law enforcement officials, into the ISE by identifying three "tracks"[427] of information sharing progress. First, the DOJ is responsible for implementing an internal reorganization strategy

Data Exchange (N-DEx) System, PoliceOne, Aug. 7, 2007, *available at* http://www.policeone.com/writers/columnists/MarkMarshall/articles/1295732/ [hereinafter Marshall].

422 *LEISP: United States Department of Justice Law Enforcement Information Sharing Program*, Department of Justice, Oct. 2005, *available at* http://www.usdoj.gov/jmd/ocio/onedoj_strategy.pdf [hereinafter *LEISP*].

423 *Ibid*.

424 *Ibid*.

425 *Assessment of Information Sharing Centers, supra* note 289.

426 Gary M. Bald, Executive Assistant Director, National Security Branch, Federal Bureau of Investigation, Remarks before the United States Senate Committee on the Judiciary, Sept 21, 2005, transcript *available at* http://www.fbi.gov/congress/congress05/bald092105.htm [hereinafter Bald].

427 *LEISP, supra* note 422.

called OneDOJ.[428] According to the guiding principles of OneDOJ, the initiative will reform and consolidate the Department's information sharing policies such that the Department may "share information among its components and present itself to law enforcement partners as a single entity for information exchange."[429] Second, the DOJ is working to build upon existing information sharing capabilities by improving, integrating, and expanding access to law enforcement databases, thereby preventing the "stovepiping" of information by independent law enforcement agencies.[430] This process will also address cultural barriers to sharing by deconstructing causes of agency mistrust and preventing information from being categorized, outside standard privacy and security policies, as "non-shareable."[431] Finally, the LEISP envisions a collaborative process by which the DOJ and SLT law enforcement officials will develop strategies to coordinate policy, privacy, and technology issues in multi-jurisdictional sharing. Progress on these three tracks is currently occurring simultaneously.[432]

In March 2006, the DOJ enhanced the abstract, policy-oriented guidance contained in the LEISP with its release of *Sharing Justice Information: A Capability Assessment Toolkit*. The *Toolkit* is a web-based program providing law enforcement agencies with practical guidelines for evaluating and improving sharing practices. Regina B. Schofield, Assistant Attorney General for the Office of Justice Programs (OJP) explained, "Information sharing initiatives are extremely complex, so agencies must constantly assess their organizational and technical capabilities."[433]

The *Toolkit* enables law enforcement agencies to assess information sharing initiatives by examining such factors as organization, management, enterprise architecture, governance, cooperation with key participants, information security and privacy policies, performance metrics, and technological capabilities.[434] The assessment mechanisms discussed by the *Toolkit* underscore the importance of "collaboration readiness," which refers to "the degree to which relationships among information users and other resources support collaboration" and collective decision-making.[435] The *Toolkit*'s emphasis on relationships and trust-building seeks to prevent cultural barriers to effective information sharing, including stovepiping, interagency mistrust, and the dominance of "need to know" procedures.[436] The guide is also designed to enable law enforcement agencies to design and implement cost-effective sharing procedures. According to Schofield, "The toolkit can save time and money while providing a necessary and user-friendly guide for justice information sharing among agencies. In some cases, an agency could complete a mini-assessment of certain system components in as little as an afternoon."[437]

The DOJ's oversight of law enforcement agencies' efforts to expand information sharing is guided by the Global Justice Information Sharing Initiative (Global), a Federal Advisory Committee (FAC) consisting of representatives of more than thirty law enforcement and judicial.[438] Global advises the Attorney General on information sharing issues, striving for "efficient sharing of data among justice entities"[439] as its principal mission. Although Global meets only twice a year, its col-

428 *Ibid.*
429 *Ibid.*
430 *Ibid.*
431 *Ibid.*
432 *Ibid.*
433 *Department of Justice Announces Information Sharing Toolkit*, US Newswire, Mar. 30, 2006.
434 Bureau of Justice Assistance, *Sharing Justice Information: A Capability Assessment Toolkit*, Aug. 2005, *available at* http://www.ctg.albany.edu/publications/guides/sharing_justice_info/sharing_justice_info.pdf [hereinafter *Dep't of Justice Announces*].
435 *Ibid.*
436 *Ibid.*
437 *Dep't of Justice Announces, supra* note 433.
438 *Global Justice Information Sharing Initiative (Global)*, U.S. Dep't of Justice-Office of Justice Programs, Information Technology Initiatives, *available at* http://www.it.ojp.gov/topic.jsp?topic_id=8.
439 *Ibid.*

lection of justice professionals and information experts provide valuable recommendations in white papers, which address both technological and strategic policy issues.[440] As Global advises the Attorney General, it highlights key issues facing the DOJ's SLT partners and provides a forum for law enforcement entities to discuss common challenges to information sharing. [441]

The DOJ's efforts to reform internal information policies and collaborate with non-federal justice entities allows for more effective coordination of sharing procedures, even if the legal framework informing those procedures varies across jurisdictions. By providing unified strategies, as well as standardized information sharing goals and assessment tools, the DOJ's initiatives are improving sharing within the law enforcement community and preparing federal and SLT justice agencies for broader integration into the ISE.

A History of Sharing

In many cases, a lack of coordination across jurisdictions and the perpetuation of Cold War "need to know" policies had prevented effective information sharing within the law enforcement community prior to the attacks of September 11, 2001. Nevertheless, the law enforcement community has had some history of sharing information on criminal investigations, an experience upon which ISE implementation policies should capitalize.

In particular, the Federal Bureau of Investigation (FBI) has reached out to state and local law enforcement officials by exchanging wants, warrants, fingerprints, and forensic data while investigating specific cases.[442] In discussing potential for increased information sharing with the Senate Judiciary Subcommittee on Immigration and Border Security, Larry A. Mefford, executive assistant director of the FBI's Counterterrorism-Counterintelligence Division acknowledged that "collection of information/intelligence has always been a core function of the FBI's investigative mission,"[443] a role that has prepared the agency for broader sharing among ISE participants.

In 1995, the FBI established Law Enforcement On-Line (LEO), a secure web-based program that has allowed for the exchange of sensitive but unclassified data among some 30,000 users representing over 17,000 local law enforcement agencies and sixty federal agencies.[444] The system, which provides a discussion forum and features interactive training sessions, supports information spanning topics on terrorism, criminal investigations, and cyber crime.[445] The FBI also relies on LEO to transmit weekly intelligence reports, which have recently been made available to fusion center analysts linked to HSIN.[446] Unlike HSIN, however, LEO has proven a more effective tool for linking federal and SLT communications. After HSIN had been launched in 2004, analysts had referred to

440 *Ibid*.

441 *Ibid*.

442 Robert J. Jordan, FBI, Testimony before the United States Senate, Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, Apr. 17, 2007, transcript at *Information Sharing Initiative*, Federal Bureau of Investigation, Apr. 17, 2007, *available at* http://www.fbi.gov/congress/congress02/jordan041702.htm [hereinafter Jordan].

443 Larry A. Mefford, Executive Assistant Director, Counterterrorism/Counterintelligence Division, FBI, Testimony before the Senate Judiciary Committee, Subcommittee on Immigration and Border Security, Sept. 23, 2003, transcript at *Improvements with Information Sharing and Watch Lists*, Federal Bureau of Investigation, Sept. 23, 2003, *available at* http://www.fbi.gov/congress/congress03/mefford092303.htm [hereinafter Mefford].

444 Willie T. Hulon, Deputy Assistant Director, Counterterrorism Division, FBI, Statement before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, July 13, 2004, transcript *available at* http://www.fbi.gov/congress/congress04/bald071304.htm [hereinafter Hulon].

445 *Ibid*.

446 Maureen A. Baginski, Executive Assistant Director, Intelligence, FBI, Statement before the House Representatives Select Committee on Homeland Security, Aug. 17, 2004, transcript *available at* http://www.fbi.gov/congress/congress04/baginski081704.htm [hereinafter Baginski].

the system as a "poor shadow of the FBI's Law Enforcement Online (LEO)."[447]

LEO is also connected to the Regional Information Sharing System (RISS), which has facilitated data exchange within the law enforcement community since 1974 and been updated to meet the evolving needs of current investigations.[448] RISS is a nationwide network that is congressionally funded and organized around six RISS centers, which emphasize the sharing of information relevant to their respective regions.[449] The network has a larger user base than LEO, connecting over 7,700 law enforcement agencies as well as nearly 75,000 officers on multiple levels of government.[450] The RISS program is managed by a National Policy Group, which considers the needs of participating agencies and develops strategies on increasing information sharing on multi-jurisdictional criminal activity.[451]

Like LEO, RISS offers users several interactive information sharing tools, including chat rooms, document archives, encrypted email, and an electronic bulletin board (RISS Leads) in a user-friendly and secure environment.[452] RISS Leads is partitioned to provide special subject-matter content on national criminal intelligence (RISS Intel) and gang-related crime (RISS Gang).[453] The RISS network enables users to connect to numerous other databases on drug-related crime and white-collar crime, which are hosted by a variety of agencies, including the U.S. Secret Service. Over time, RISS has undergone numerous expansions and now offers a sophisticated mechanism for sharing data pertaining to drug trafficking, cyber crime, gangs, "emerging criminal groups," as well as terrorism.[454]

By linking thousands of law enforcement and criminal justice officials to a nationwide network, the longstanding RISS program represents a valuable asset to the ISE. Donald F. Kennedy, executive director of the New England State Police Information Network, one of the six regional centers participating in RISS, commented, "In the aftermath of 9/11, RISS recognized the critical need for timely exchange of national security and terrorist threat information, not only among law enforcement officials but to all first responders and officials involved in homeland security."[455] To advance broader information sharing, RISS established the Automated Trusted Information Exchange (ATIX) in 2003. Kennedy explained that ATIX provides "a communication system that allows first responders, critical infrastructure personnel, and other public safety personnel including firefighters and public utility and school personnel and local, state, and federal law enforcement to share terrorism and homeland security information in a secure, real-time environment." ATIX's effectiveness was recognized promptly and in 2004, ATIX was selected as the "official system for secure communication and information sharing" for the G8 Summit.[456]

The online networks LEO and RISS have proven efficient, successful, and worthy of integration into the ISE.[457] LEO and RISS have been particularly useful given that DHS' more recent sharing initiative, the HSIN, has failed to adequately link SLT officials and avoid cross-database duplication. At the same time, officials have recognized that many policy-oriented data sharing initiatives developed by the law enforcement community in the pre-9/11 period have been limited in scope. For instance, Larry A. Mefford, executive assis-

447 *Fixing the Homeland Security Information Network, supra* note 353.
448 *Assessment of Information Sharing Centers, supra* note 289.
449 *DHS Security Information Network*, CQ Congressional Testimony, May 10, 2007 [hereinafter *DHS Security Information Network*].
450 *Ibid.*
451 *Ibid.*
452 *DHS Security Information Network, supra* note 449.
453 *Ibid.*
454 *Ibid.*
455 *Ibid.*
456 *Ibid.*
457 Baginski, *supra* note 446.

tant director of the FBI's Counterterrorism-Counterintelligence Division, pointed out that aside from LEO and RISS, procedures for sharing information to enhance criminal investigations has traditionally been "case oriented."[458] Rather than an "enterprise-wide activity" of the nature that the ISE seeks to establish, law enforcement information sharing has previously focused on particular investigative missions. Even as late as mid-2002, sharing was limited by the viewpoint of many FBI officials that "need to know" policies were intertwined with adequate information security. In many cases, the position that "need to know" access controls were necessary to maintain the integrity of law enforcement information resulted in a great amount of data being categorized as "nonshareable"[459] by independent agencies. Still, LEO and RISS represent valuable tools for expanding information exchange and integrating sharing practices into daily law enforcement operations.

FBI Initiatives Improve Existing Sharing Procedures

Since 9/11, the FBI has aggressively advanced its capability to gather intelligence, investigate emerging terror threats, and manage information sharing initiatives. Robert J. Jordan, head of the FBI's Information Sharing Task Force, has commented that the FBI "is an organization in change" that has seen "massive shifts in…resource deployments,…missions and priorities to better reflect the post-9/11 realities."[460]

The FBI's capacity to improve terrorism information sharing is linked to the agency's recent internal organizational reform, which added branches to manage national security issues, including intelligence/counterintelligence, counterterrorism, and weapons of mass destruction.[461] Information policies have also received fresh guidance from the recently appointed Chief Information Officer and the new security division, which concentrates on information security.[462] Though the FBI has always carried dual functions as an intelligence and investigative agency, the organization has redoubled its intelligence efforts by adding an Office of Intelligence charged with maintaining a "vigorous and fluid flow" of intelligence information within the law enforcement community and with the IC.[463] The FBI is also devoting more time and resources to the development and dissemination of Intelligence Information Reports (IIRs), Intelligence Assessments (IAs), and Intelligence Bulletins (IBs) on national security and terrorist threats.[464]

Enactment of the USA PATRIOT Act has greatly expanded the FBI's information sharing capabilities. Deconstructing the "wall" of previous restrictions on the sharing of law enforcement information, the legislation enables the FBI to exchange data and cooperate more closely with the IC. As Steven C. McCraw, FBI assistant director, explained to the House Select Subcommittee on Homeland Security in 2003, the framers of the USA PATRIOT Act recognized that "the benefits of sharing information far exceeds risks" and that "transparency in…knowledge of terrorist threats" is one of the most critical counterterrorism tools.[465] McCraw also explained, "In today's threat environment, cooperation rather than competition must be the guiding principle."[466] The USA PATRIOT Act, as well as revised Attorney General Guidelines,[467] promote collaboration among law enforcement and intelligence agencies by permitting, in some cases for the first time, the sharing

458 Mefford, *supra* note 443.
459 *LEISP, supra* note 422.
460 Jordan, *supra* note 442.
461 Bald, *supra* note 426.
462 Jordan, *supra* note 442.
463 *Ibid*.
464 *Ibid*.
465 Steven, C. McCraw, Assistant Director, FBI, Testimony before the House Select Committee on Homeland Security Subcommittee, July 24, 2003, transcript at, *Intelligence and Counterterrorism*, Federal Bureau of Investigation, July 24, 2003, *available at* http://www.fbi.gov/congress/congress03/mccraw072403.htm [hereinafter McCraw].
466 *Ibid*.
467 Mefford, *supra* note 443.

of grand jury information and foreign intelligence information acquired in the course of criminal investigations.

Since 9/11, the FBI has adopted a vigorous approach to increasing sharing and has taken several important steps to collaborate with a variety of ISE participants. Many of the FBI's current information sharing initiatives stem from its recent organizational transformation and amplified emphasis on intelligence and counterterrorism functions.[468] As Maureen A. Baginski, FBI executive assistant director for intelligence, remarked, the FBI's information sharing initiatives is driven by the "core guiding principle…that intelligence and law enforcement operations must be integrated."[469]

As part of the DOJ's LEISP, the FBI has released a National Information Sharing Strategy (NISS), which coordinates law enforcement collaboration and contributions to ISE implementation.[470] NISS outlines a three-track technical plan for increasing law enforcement information sharing, which consists of use of LEO, as well as two new databases, National Data Exchange (N-DEx) and Regional Data Exchange (R-DEx).

N-DEx, a recently developed network nearing fully operational status, is an investigative tool that enables law enforcement officers to compare their cases to similar incidents being examined by other agencies. FBI Chief Information Officer (CIO) Zalmai Azmi stated, "The development and deployment of N-DEx will provide nationwide capability to share information derived from incident, arrest and event reports. This will expedite coordination across law enforcement so that we can remain one step ahead of the criminals and terrorists despite jurisdictional boundaries."[471] By compiling information on suspicious activity gathered by law enforcement officials across the nation, N-DEx will facilitate the process of making analytical connections that had been lacking before 9/11. As SLT officers will be the primary users of the system, the N-DEx "Statement of Requirements" largely reflects the views of local officers and organizations, such as the International Association of Chiefs of Police, on information sharing.[472] At the same time, however, federal agencies such as ATF, DEA, Bureau of Prisons, FBI, and U.S. Marshals will contribute to the database supported by N-DEx.[473]

Though programs like LEO and RISS already link law enforcement officials across jurisdictions, N-DEx improves upon earlier information sharing efforts by integrating data. Mark A. Marshall, Chief of Police of Smithfield, Virginia, has assessed N-DEx as a highly useful and efficient data exchange system. He commented, "Participation in N-DEx will complement and expand those capabilities, using a model of incident data aggregation that did not exist on a national scale. N-DEx will provide well-defined integration points which allow for inclusion of…already established groups, technologies, etc. into the broader N-DEx information sharing architecture."[474]

The Regional Data Exchange, or R-DEx, which was launched in St. Louis in February 2005, provides a bank of investigative data, including information on "individuals, vehicles, weapons, addresses, [and] phone numbers."[475] In addition, the network's analytical assistance tools also enable investigators to construct maps and examine geographical information relevant to their cases.[476] The program provides connectivity to information stored in several other databases, such as the Naval Criminal Investigative Services' Law Enforcement Information Exchange (LinX), a law

468 Baginski, *supra* note 446.
469 *Ibid*.
470 *FBI Announces Contract Award in Information Sharing Program*, States News Service, Feb. 16, 2007 [hereinafter *FBI Announces*].
471 *Ibid*.
472 Marshall, *supra* note 421.
473 *FBI Announces, supra* note 470.
474 Marshall, *supra* note 421.
475 Jordan, *supra* note 442.
476 *Ibid*.

enforcement network developed and maintained by the city of Seattle.[477]

Reliance on R-DEx has achieved early successes. The FBI, the Illinois State Police, the Missouri State Highway Patrol, the St. Louis Metropolitan Police, the St. Louis County Police, and the St. Clair County (Illinois) Sheriff's Department all access R-DEx on a regular basis to assist each other's investigations.[478] Like N-DEx, the R-DEx system provides a useful mechanism for coordinating investigations that are inter-jurisdictional in nature. Increased use of the system encourages law enforcement officials to overcome barriers to sharing by integrating sharing and investigation-enhancing tools into daily procedures.[479] By providing access to highly specific information on items that are frequently the subject of investigations, R-DEx also advances the FBI and DOJ's broad goal of ensuring that law enforcement agencies "share by rule and withhold by exception."[480] Use of both N-DEx and R-DEx greatly enhances law enforcement officials' ability to integrate data, make appropriate deductions, and notify SLT and federal partners about potential terrorist threats.

The Terrorist Screening Center (TSC)

Outside the information technology initiatives launched by NISS, the FBI has endeavored to boost information sharing by improving operations at the Terrorist Screening Center (TSC). An information sharing institution launched shortly after the 9/11 attacks, the TSC is an interagency organization that consolidates information on suspected terrorists into a Terrorist Screening Database (TSDB) and offers a 24/7 real-time terrorism watch to law enforcement and intelligence agencies.[481] The Center was established under Homeland Security Presidential Directive (HSPD)-6 and is subject to federal privacy restrictions. Representatives from the FBI, as well as the DOJ, DHS, DOS, and Treasury Department contribute to the TSC's operations.[482]

The TSC currently manages a Terrorism Watch List (TWL), which is intended to serve as the FBI's "single, integrated listing of individuals of investigative interest."[483] The TWC contains names and information about individuals falling into one of three categories: (1) individuals against whom criminal charges or indictments have been issued; (2) names and information about individuals "of investigative interest" to the FBI; and (3) names of individuals, offered by intelligence agencies or foreign governments, who are suspected of engaging in terrorist activities.[484] The TSC also manages Interpol resources and data on consular issues, border security, flight lists, warrants, gangs, and fugitives.[485] Information handled by the TSC can be used to notify law enforcement officials if individuals of interest to terrorism investigations enter their respective jurisdictions.[486] The TSC also permits law enforcement officials to run "name checks" and permits terrorist screenings to be conducted for visa applicants.[487]

According to FBI Director Robert Mueller, "What's different about the TSC is the ability to make…[terrorism] information available in real time, constantly updated, 24 hours a day and

477 *More Data for FBI's National Information Sharing System,* Gov't Technology Beta, June 29, 2006, *available at* http://www.govtech.com/gt/articles/100047.
478 Jordan, *supra* note 442.
479 *Ibid*.
480 *Ibid*.
481 Mefford, *supra* note 443.
482 Donna A. Bucella, Director, Terrorist Screening Center, Statement before the House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations, transcript at, Federal Bureau of Investigation, *available at* http://www.fbi.gov/congress/congress04/bucella071304.htm [hereinafter Bucella].
483 Jordan, *supra* note 442.
484 *Ibid*.
485 Bucella, *supra* note 482.
486 Jordan, *supra* note 442.
487 Press Release, Office of Homeland Security, New Terrorist Screening Center Established, Sept. 16, 2003, *available at* http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html.

across the board."[488] Mueller added, "By providing this around-the-clock service to anti-terrorist screeners throughout the federal government, the new Center will ensure not only that those who need it will have access to the best, most current information, but they will also have access to on-call experts who can support them in taking immediate and appropriate action to stop terrorists and prevent attacks at any hour of the day or night."[489]

The TSC, however, has raised questions about privacy and the reliability of information that results in an individual's name being entered in the TSDB. Under HSPD-6, only individuals "who are known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism" are suitable for inclusion in the TSDB.[490] Still, HSPD-6 standards are vague and, in order for the TSC to function effectively, it cannot inform an individual as to whether he or she has been added to the database. Some concerns are alleviated by the requirement that names be removed from the TSDB as soon as an individual no longer meets HSPD-6 standards. Additionally, since TSC is an interagency organization, it may only handle information constitutionally collected by its member agencies, which are subject to restrictions designed to protect privacy and civil liberties.[491]

In a June 2005 study, the Department of Justice's Office of the Inspector General (DOJ OIG) reported that the TSC has had some difficulties ensuring the accuracy and comprehensiveness of its database.[492] Some information included in the database lacked tagging codes and in other cases, the TSDB was missing information on known domestic and international terrorists.[493] The OIG recommended that the TSC review its holdings to rectify problems created by "missing, conflicting, or duplicate information."[494] The report also suggested the adoption of improved search engines and information assurance policies.[495]

On the whole, the TSC has received a mixture of criticism and praise. Some Center officials claim that the TSC is "well-positioned to assist communications between agencies,"[496] despite critics' complaints that the TSC is "riddled with problems…management deficiencies, immature information technology, and high personnel turnover."[497] Many of the TSC's inadequacies appear rectifiable through enhanced personnel training, improved oversight and management, as well as the development of procedures on data quality control and information updates. Though the TSC must continue working to improve information assurance and accuracy, the multi-agency endeavor represents a considerable step toward seamless information sharing on suspected terrorists.

Information Sharing Working Groups

The FBI contributes representatives to a number of interagency working groups seeking to enhance sharing across the ISE's participating communities. The Information Sharing Policy Group (ISPG), created by the FBI in 2004, advises policy on both federal/SLT law enforcement information sharing as well as efforts to develop a more trusted partnership with intelligence officials.[498] In September 2005, the FBI completed an Intelligence Policy Manual that builds upon the ISPG's work.

488 *Ibid.*
489 *Ibid.*
490 Federal Bureau of Investigation, Counterterrorism-Terrorist Screening Center, http://www.fbi.gov/terrorinfo/counterrorism/faqs.htm (last visited Jan. 27, 2008).
491 *Ibid.*
492 U.S. Department of Justice, Office of the Inspector General, Audit Division, *Review of the Terrorist Screening Center*, June 2005, http://www.usdoj.gov/oig/reports/FBI/a0527/final.pdf.
493 *Ibid.*
494 *Ibid.*
495 *Ibid.*
496 Bucella, *supra* note 482.
497 Chris Strohm, *Terrorist Screening Center Plagued by Deficiencies, Audit Finds*, Gov't Executive, June 14, 2005, *available at* http://www.govexec.com/dailyfed/0605/061405c1.htm.
498 Bald, *supra* note 426.

The Manual guides law enforcement and intelligence agencies on maintaining equilibrium between "need to share" policies and information security strategies.[499]

The FBI is also a member and chair of the Justice Intelligence Coordinating Council (JICC). Created by the Attorney General in 2004, the JICC examines methods for strengthening and coordinating the DOJ's intelligence functions. The JICC provides recommendations on collaboration with the IC, examines emerging information technology, and improves strategies set forth in the LEISP. Additionally, the group addresses technical issues and contributes to the development of intelligence sharing training programs.[500]

Finally, the FBI participates in the GLOBAL Intelligence Working Group and the GLOBAL Criminal Intelligence Coordinating Council (CICC). These bodies, both established in 2004, develop policies guiding the work of law enforcement officials stationed at state and local fusion centers.[501]

Sharing with Defense Partners

The FBI's robust sharing initiatives extend to partnerships with defense and foreign ISE participants. In 2003, the FBI created secure information sharing web-pages, where DoD officials could post Top Secret and Secret information.[502] To foster cooperation with the defense community, the FBI shares biometric data, including fingerprints, photographs, and biographical information on detainees and enemy prisoners of war, to military officials.[503] The FBI's Foreign Terrorist Tracking Task Force (FTTTF) also provides analytical support to DoD Counterintelligence Field Activity (CIFA). The DoD and FBI collaborate as members of the Terrorist Explosive Device Analytical Center, which manages forensic data and provides the military with useful information about improvised explosive devices (IEDs).[504]

Close FBI and DoD collaboration is also achieved through the placement of Special Agent Bomb Technicians (SABTs) and FBI investigators with U.S. troops in Iraq and Afghanistan.[505] FBI investigators stationed abroad have contributed to the development of the Intelligence and Terrorist Photograph Identification Database (INTREPID), which contains over 12,000 images and videos of suspected terrorists.[506] INTREPID has greatly aided the DoD's counterterrorism and counterinsurgency missions and military personnel to regularly update the system by providing images acquired during operations in Afghanistan, Iraq, and Guantanamo Bay, Cuba.[507]

Expansion of Joint-Terrorism Task Forces (JTTFs)

One of the FBI's most significant interagency sharing initiatives involves the increased employment of Joint Terrorism Task Forces (JTTFs). These organizations share and analyze classified information to coordinate federal and SLT counterterrorism efforts.

Although created before 9/11, the FBI has successfully adopted them to deal with post-9/11 terrorist threats within the United States as part of the Bureau's own restructuring to focus on preventing terrorism and other national security threats as well as prosecuting perpetrators of these acts and other criminals after the fact. Most significantly, in November 2001, Director Robert S. Mueller oversaw a major reorganization that established several new offices designed to enhance the FBI's information sharing capacities in the area of counterterrorism. These issues included several related to information technology, intelligence, records management, and law

499 *Ibid.*
500 *Ibid.*
501 *Ibid.*
502 McCraw, *supra* note 465.
503 Bald, *supra* note 426.
504 *Ibid.*
505 *Ibid.*
506 *Ibid.*
507 *Ibid.*

enforcement coordination with state and local partners.

The FBI established first JTTF in New York City in 1980 following a surge in local bank robberies. After the new structure proved successful in enhancing cooperation between the FBI and the New York Police Department (NYPD), the FBI expanded the use of JTTFs, in part to respond to terrorist threats.[508] The FBI defines terrorism as any unlawful use of force or violence, by an individual or group of individuals, against persons or property to intimidate or coerce a government, civilians, or any of the above, to gain political or social objectives.[509]

The JTTFs now regularly include full-time participation of investigators from 17 Federal, state and local law enforcement agencies. The federal agencies included the Immigration and Naturalization Service (INS), Marshal's Service, Secret Service, FAA, Customs Service, ATF, State Department, Postal Inspection Service, IRS, and the U.S. Park Police. Numerous state and local law enforcement agencies are likewise full-time members of JTTFs.[510]

JTTFs provide training to their participants, host dialogues to support case-specific investigations, and foster the sharing of intelligence. According to Robert J. Jordan, head of the FBI Information Sharing Task Force, "Years of experience have demonstrated that Joint Terrorism Task Forces (JTTFs) have proven to be one of the most effective methods of unifying federal, state and local law enforcement efforts to prevent and investigate terrorist activity by ensuring that all levels of law enforcement are fully benefiting from the information possessed by each."[511]

JTTFs have significantly aided investigations of the 1993 World Trade Center bombing, crimes committed by the Ku Klux Klan, financial transactions by Hamas through U.S. Islamic charities, and the activities of homegrown Hizbollah terrorist cells and the Palestine Islamic Jihad within the United States.[512] JTTFs also played a role in securing the conviction of Ramzi Yousef and Eyad Mahamoud Ismail for conspiracy in the bombing of the World Trade Center as well as in the arrest and prosecution of Richard Reid, charged with attempting to destroy a civilian passenger plane in mid-flight over the Atlantic.[513] More recently, the JTTFs helped secure the extradition of Syed Hashmi from the United Kingdom for providing al-Qa'eda with material support and helped detect an alleged plot to bomb John F. Kennedy International Airport.[514] The JTTFs also regularly coordinate security preparations for major special events such as the 2002 Winter Olympics, the NFL Super Bowls, and recurring national holidays (e.g., Independence Day) and international meetings (e.g., the annual International Monetary Fund conference).

Regional Terrorism Task Forces (RTTFs) supplement the work of the JTTFs. These bodies have the same objective of enhancing information sharing between the FBI and other public bodies, but are less institutionalized than the JTTFs. They typically involve semi-annual meetings on counterterrorism issues among law enforcement personnel from the FBI and other federal, state, and local law enforcement personnel.[515]

508 Nevada Emergency Operations & Notification Network, Joint Terrorism Task Force (JTTF), NEONN.org, *available at* http://neonn.org/index.cfm/MenuItemID/224.htm (last visited Jan. 27, 2008) [hereinafter Nevada Emergency Operations].

509 *Ibid*.

510 Jordan, *supra* note 442.

511 *Ibid*.

512 Office of the Inspector General, *The Department of Justice's Terrorism Task Forces*, June 2005, *available at* http://www.usdoj.gov/oig/reports/plus/e0507/background.htm.

513 Nevada Emergency Operations, *supra* note 508.

514 Press Release, Department of Justice, Four Individuals Charged in Plot to Bomb John F. Kennedy International Airport, June 2, 2007, *available at* http://newyork.fbi.gov/dojpressrel/pressrel07/plot060207.pdf; Press Release, Federal Bureau of Investigation New York Division, United States Announces First Extradition form United Kingdom on Terrorism Charges, May 26, 2007, *available at* http://newyork.fbi.gov/dojpressrel/pressrel07/extradition052607.htm.

515 Jordan, *supra* note 442.

A National Joint Terrorism Task Force (NJTTF), which is based at the Strategic Information and Operations Center of the FBI Headquarters, serves as venue for exchanging information among federal and SLT entities belonging to the intelligence, law enforcement, and public safety communities.[516] The NJTTF originated immediately after 9/11 as an ad hoc group of representatives from federal agencies involved in the counterterrorism mission. The participating federal agencies now include representatives from the intelligence community, the Nuclear Regulatory Commission, the Railroad Police, and from the Departments of Homeland Security, Defense, Justice, Treasury, Commerce, Transportation, Energy, State, and the Interior.[517]

The NJTTF currently hosts electronic terrorism databases and daily intelligence conferences, integrates and analyzes data to achieve comprehensive assessments of national terror threats.[518] As a result, besides providing administrative, logistical, and training support to the JTTFs, the NJTTF effectively serves as a "fusion" center for intelligence collected by JTTFs.[519]

Eleven JTTFs existed in 1996.[520] After 9/11, the FBI devoted considerable resources to increase this number to over one hundred. For example, the FBI increased its budget for JTTF-related funding from $216 million in FY 2003 to $375.2 million in FY 2005.[521] The New York JTTF remains the largest, with approximately 500 investigators, analysts, and other experts from over forty different public sector agencies among the region.

In line with the FBI's new post-9/11 focus on detecting national security threats before they mature, the Bureau has augmented the ability of the JTTFs to share information with the intelligence community by tasking a Special Agent or Intelligence Analyst within each JTTF for this purpose.[522] These officials are responsible for the collection of "raw" intelligence data "for the entire national security community," which includes SLT law enforcement officials and JTTF participants.[523]

The FBI has also established Field Intelligence Groups (FIGs), in each of its fifty-six field offices, to enhance the JTTFs. They include Intelligence Analysts (IAs), Special Agents (SAs), Language Analysts (LAs), and Surveillance Specialists.[524] Their purpose is to ensure that JTTFs support federal initiatives to exchange terrorism information with the IC.[525] They also provide guidance to JTTFs on the dissemination of JTTF work products to state and local fusion centers. Willie T. Hulon, the FBI's Deputy Assistant Director of the Counterterrorism Division, explained that, "The FIGs play a major role in ensuring that from now on, 'we know what we know' and we tell others in the Intelligence Community and our federal, state, local, and tribal law enforcement partners 'what we know.'"[526]

For law enforcement officials unable to participate in JTTFs, the FBI offers special training programs.[527] Many attempt to share the latest counterterrorism tradecraft employed by the FBI. They provide additional evidence that the FBI considers that all SLT law enforcement officers, including those outside major urban areas, have a critical role to play in collecting and disseminating terrorism information. Since 2003, more than 27,000 local police officers have benefited from expanded FBI efforts to provide up-to-date counterterrorism training.[528]

516 Baginski, *supra* note 446.
517 Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement to Committee on Senate Judiciary, CQ Congressional Testimony, Dec. 6, 2006.
518 Bald, *supra* note 426.
519 Baginski, *supra* note 446.
520 Jordan, *supra* note 442.
521 *The Department of Justice's Terrorism Task Forces Evaluation & Inspections Report I-2005-007*, Office of the Inspector General, June 2005, *available at* http://www.usdoj.gov/oig/reports/plus/e0507/background.htm [hereinafter *Department of Justice's Terrorism Task Forces*].
522 Baginski, *supra* note 446.
523 *Ibid*.
524 *Intelligence Revision, supra* note 72.
525 Hulon, *supra* note 444.
526 *Ibid*.
527 McCraw, *supra* note 465.
528 *Ibid*.

The Office of the Inspector General (OIG) at the Department of Justice has identified 28 recommendations that the DOJ could take to improve the operations of the department's various counterterrorism task forces and councils. Several appear especially relevant to improving information-sharing within the JTTF process.[529]

First, the FBI needs to develop more national orientation and training plans for JTTF members to ensure a certain degree of uniform preparedness and to counter perceptions that FBI members receive privileged access to training opportunities.

Second, the JTTF network needs to ensure that it more effectively extends to law enforcement personnel working in remote areas so mutual exchange of data with these communities occurs. (Terrorists might perceive such gaps as opportunities to establish safe havens.)

Third, as with many government programs, the FBI has yet to develop optimal measures of effectiveness to evaluate the work of JTTFs. Inputs in terms of dollars spent or personnel assigned to JTTFs can easily be measured, but assessing the precise contribution of JTTFs is difficult given the multidimensional nature of the terrorist challenge and the fact that the most important success—preventing a terrorist incident—is by definition a non-event.

Fourth, some JTTFs had inadequate administrative and analytical support, high turnover in task force leadership, or exceeded their authorized staffing levels. Some of these problems resulted from the urgent need to expand the JTTF program after 9/11, but the recent stabilization in the growth of the JTTFs should allow the FBI to address some of these problems more comprehensively. Rather than increase the number of JTTF further, the FBI might find it optimal to meet authorized staffing levels of existing JTTFs. The current practice of diverting personnel from other FBI programs, such as those designed to counter narcotics trafficking or white-collar crime, risks weakening the U.S. ability to achieve those important objectives.

In terms of meeting ISE objectives, it is essential for FBI personnel to have access to the most advanced computer and information technologies, both at headquarter facilities and more remote locations. All JTTF members need software capable of searching information that might exist in the databases of all the participating agencies. The OIG found that JTTF participants sometimes had to waste time and return to their parent agencies to perform data searches.

Fifth, the OIG concluded that the Drug Enforcement Administration (DEA) needed to increase its involvement in the JTTF process given the connection between narcotics trafficking and terrorism. The cases of Columbia and Afghanistan show most vividly how terrorists can use illicit drug dealing to fund their operations and weaken government authority.

One original ISE-related problem that appears to have been largely overcome is the need to ensure that state and local law enforcement personnel receive security clearances at the level of their FBI counterparts. Inequities in this area were common immediately after 9/11, but during the last few years increasing numbers of non-USG personnel have received adequate security clearances after the standard lengthy background investigations.

Non-Government Actors

The ISE Implementation Plan envisions a critical role for non-government actors in information sharing. Establishing a "distributed, decentralized, and coordinated"[530] information flow requires integration of not only SLT governments, but also private sector entities, which play an essential role in protecting the nation's critical infrastructure.

529 *Department of Justice's Terrorism Task Forces, supra* note 521.

530 *ISE Implementation Plan, supra* note 24.

It is likewise important to consider the impact of non-profit entities on the development of information sharing strategies. One non-profit organization, the Markle Foundation, has made notable research contributions and influenced the development of the ISE's legal framework.

The Private Sector

Private sector participation is essential to success of the ISE. Over eighty percent of the nation's critical infrastructure is currently owned and controlled by private industry.[531] The increasing sophistication of terrorist activities also calls for greater government reliance upon emerging technology and the capabilities of private sector experts.[532] As the international presence of many large private sector entities requires them to collect information to ensure the security of their operations worldwide, their data offers a key asset to government partners. For the private sector, robust information exchange with the government represents an opportunity to better assess potential threats, develop needed security technology, and efficiently allocate resources for the protection of the nation's critical infrastructure.[533]

U.S. Chamber of Commerce counsel Carol Hallet has asserted that private businesses, many of which have apportioned a considerable amount of funds to protect their employees and operations from terrorism since 9/11, are "eager to share"[534] information with government partners. As with vertical federal/SLT sharing, however, the success of information exchange between the public and private sectors largely depends upon participants' ability to develop trusted relationships. An effective ISE must foster a collaborative approach to protecting critical infrastructure that provides adequate communications pathways as well as training opportunities. Participants must engage in a genuine bilateral information exchange whereby government entities develop a more comprehensive understanding of infrastructure vulnerabilities and businesses receive "actionable, timely and threat-specific information."[535]

A Framework for Private/Public Sector Partnerships

In Homeland Security Presidential Directive-7(HSPD), issued in December 2003, President Bush emphasized that "critical infrastructure and key resources provide the essential services that underpin American society."[536] He therefore ordered that federal departments and agencies "identify and prioritize"[537] these resources in order to "deter, mitigate, or neutralize potential attacks."[538] To implement HSPD-7, DHS developed the National Infrastructure Protection Plan (NIPP), which was released in 2006. The NIPP, which details cooperatives strategies for improving the security of critical infrastructure and key resources, also provides a framework for public and private sector homeland security information sharing.

Developed through collaboration with private sector partners, the NIPP recognizes private sector owners and operators as "the first line of defense" for critical infrastructure and key resources.[539] The NIPP therefore considers two-way information sharing between the government and private industries the most efficient mechanism for as-

531 *Ibid.*

532 *The Private Sector's Role in Building the Intelligence Community of the 21st Century: Increased Partnering with Industry to Maintain America's Edge*, PR Newswire, Mar. 3, 2005 [hereinafter *The Private Sector's Role*].

533 *U.S. Chamber of Commerce National Security Business Forum: John Negroponte, Director of National Intelligence*, Federal News Service, July 10, 2006.

534 *Ibid.*

535 *Ibid.*

536 Press Release, President George W. Bush, Homeland Security Presidential Directive/HSPD-7, Dec. 17, 2003, *available at* http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

537 *Ibid.*

538 *Ibid.*

539 *National Infrastructure Protection Plan*, Department of Homeland Security, 2006, *available at* www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf [hereinafter *National Infrastructure Plan*].

sessing risks, allocating resources, disseminating security notifications, and improving public/private sector coordination.[540] While recognizing the need for confidentiality in business operations, the NIPP emphasizes the importance of integrating information collected by government and private entities to maximize situational awareness.

Under the NIPP, information sharing between public and private sector partners relies upon a network approach coordinated by HSIN, the web-based data exchange portal also used to facilitate vertical sharing between federal and SLT entities. This approach allows for "multidirectional" sharing and ensures that data is exchanged in a secure environment. The NIPP requires that "strategic and specific threat assessments, threat warnings, incident reports, all-hazards impact assessments, and best practices" be through HSIN and shared between government and private sector actors.[541]

The strategies contained in the NIPP also depend upon several institutions that facilitate information exchange between the public and private sectors. Advisory councils, such as the Critical Infrastructure Partnership Advisory Council (CIPAC) and the Homeland Security Advisory Council (HSAC), pool private and public sector expertise and offer recommendations on improving collaborative efforts to protect critical infrastructure.[542] Additionally, the NIPP highlights the role of Information Sharing and Analysis Centers (ISACs), whose primary mission is to offer secure data exchange platforms that facilitate the collection and analysis of security threat information.[543] The information handled by ISACs is largely provided by authorized private sector participants, who may also receive threat alerts from ISACs.[544] However, ISACs' analysis specialists also receive data from other entities, including law enforcement agencies, technology specialists, and security associations.[545] Much like fusion centers, ISACs work to integrate numerous sources of information in order to develop a better understanding of emerging security threats.

Currently, ISACs address fourteen critical infrastructures, including communications, electricity, emergency management and response, financial services, highway, information technology, public transit, surface transportation, and water.[546] They are assisted by Sector Coordinating Councils (SCCs), which organize and direct information sharing processes within particular sectors, as well as assist sharing across industries and with the federal government.[547] SCCs encourage a robust flow of information on security threats, vulnerabilities, and incidents while also providing policy recommendations to improve critical infrastructure protection and emergency preparedness.[548] The work of both ISACs and SCCs is supplemented by the National Infrastructure Coordination Center (NICC). Identified by the NIPP as one of the "primary conduits for sharing terrorism information today,"[549] the DHS institution is responsible for synchronizing public and private sector information in response to a security incident. NICC brings together industry experts and members of ISACs in order to integrate information collected by the fourteen critical infrastructure sectors.[550]

In addition to the strategies outlined by the NIPP, information sharing between the public and private sectors receives considerable support from InfraGard, a program established by the FBI in

540 *Ibid.*
541 *Ibid.*
542 *Ibid.*
543 *Ibid.*
544 World Wide/Information Sharing and Analysis Center, *available at* http://www.wwisac.com (last visited Jan. 27, 2008).
545 *Ibid.*
546 ISACCouncil.org, Representing the Combined ISAC Council Members, *available at* www.isaccouncil.org/about (last visited Jan. 27, 2008).
547 Communications Sector Coordinating Council (CSCC), *available at* http://www.commscc.org (last visited Jan. 27, 2008).
548 *Ibid.*
549 *National Infrastructure Protection Plan, supra* note 539.
550 *Ibid.*

1996 at its Cleveland field office.[551] Originally developed to assist cyber crime investigations through collaboration with information technology experts and academia, InfraGard, which has cultivated a trusted relationship between law enforcement agencies and private sector entities, has evolved since 9/11 to enhance FBI investigations on intelligence and security matters. InfraGard Chapters located across the nation provide resources for information collection and analysis, training opportunities, and forum discussions to foster an energetic discourse between law enforcement and private sector partners. The InfraGard program also provides a secure web-based communications platform to enhance information sharing among its participants. According to the FBI, InfraGard advances "ongoing dialogue and timely communication" between the FBI and the private sector, exchanging information on counterterrorism, cyber crime, critical infrastructure vulnerabilities, and threat alerts.[552]

Moving Forward

InfraGard and the NIPP provide an important framework for the protection of critical infrastructure that is expected be strengthened via ISE implementation. In the short-term, however, improving the sharing strategies and mechanisms outlined in the NIPP should remain a priority for DHS. Since the NIPP relies heavily upon HSIN for data collection and integration, DHS must work persistently to improve the sharing network, which has suffered from hurried implementation, data duplication and omissions, and ineffective management. DHS must likewise encourage more robust private sector collaboration with ISACs. According to Andrew Howells, former vice-president of homeland security for the U.S. Chamber of Commerce, many private sector entities have not fully capitalized on opportunities for information sharing with ISACs. "They never…figured out their relationship" with ISACs, he commented.[553] Because the ISACs and SSCs are divided into separate groups representing each of fourteen critical infrastructures, information sharing efforts have occasionally resulted in duplicated efforts.[554]

Implementation of the ISE, however, should improve private/public sector partnerships by providing more effective leadership and clearer goals to coordinate private sector sharing initiatives. Private sector representatives have already been incorporated as participants in the ISE management structure through the creation of the ISC's Private Sector Subcommittee, which consists of private sector experts and is co-chaired by the DOJ and DHS.[555] The Subcommittee provides recommendations and updated strategies for improving the integration of private sector data into government processes and enhancing implementation of the sharing procedures envisioned by the NIPP.[556]

The ISE Implementation Plan will also enhance public/private sector relationships by requiring the establishment of liability and antitrust protection policies. By alleviating industry concerns, these policies enable private sector and government partners to build needed trust for vigorous information sharing. The strategies contained in the ISE Implementation Plan, as well as the ongoing efforts of the ISC and PM-ISE to advance information sharing, are expected to enhance situational awareness of both government and private entities and facilitate the dissemination of information necessary to protect the nation's critical infrastructure.

New Information Technology

In addition to providing the government with needed information on critical infrastructure threats and vulnerabilities, the private sector makes an

551 InfraGard: Guarding the Nation's Infrastructure, *available at* http://www.infragard.net/index.htm (last visited Jan. 27, 2008).
552 *Ibid.*
553 *FBI Announces, supra* note 470.
554 *National Infrastructure Protection Plan, supra* note 539.
555 *Ibid.*
556 *Ibid.*

important contribution to the ISE through the development of innovative information technology. As previously discussed, Xythos has created software improving the DoD's communications and situational awareness. Similarly, Raytheon has enhanced sharing within the law enforcement community through the development of the N-DEx information system.[557] Several other companies have likewise played a significant role in enhancing the information capabilities of the ISE's federal and SLT participants.

AEP Networks, which specializes in information security, has developed a number of applications that facilitate homeland security information sharing. At the 2005 All Hazards Forum Conference and Exhibition in Baltimore, Maryland, AEP Networks unveiled several technologies that improve access control and maintain the integrity of information shared on web-based portals.[558] AEP Networks' contributions include AEP SmartGate, a program designed for "large-scale distributed information sharing environments" that manages data access across several servers; AEP Net, which relies upon encryption procedures to provide "high data confidentiality and source authentication" for LAN and WAN networks; and AEP Keyper, which allows for secure data storage. AEP is also developing improved identity-based access control technologies. Some of AEP's developments have already been selected for use by ISE participants. For instance, the law enforcement community has successfully relied on AEP applications to ensure data security on the Regional Information Sharing Systems Network (RISS).[559]

Two other companies, General Dynamics Advanced Information Systems and Jabber, Inc. have collaborated to provide "secure and scalable enterprise messaging and presence solutions" to the defense, intelligence, and homeland security communities.[560] Their technology products, currently offered by Jabber, Inc., include the Jabber Extensible Communications Platform (Jabber XCP), a programmable Extensible Markup Language (XML) that augments messaging capabilities. Jabber XCP is said to "weave applications, networks, devices, multi-media and protocols together into a real-time information sharing environment, where context is dynamically added to new and continuous data streams." Jabber XCP also offers Extensible Messaging and Presence Protocol (XMPP), an application which has received approval from the Internet Engineering Task Force (IETF) for instant messaging at the DoD and other federal departments and agencies. Mark Kusiak, Director of Homeland Security and Information Assurance at General Dynamics Advanced Information Systems commented, "XMPP has gained significant traction within the federal government as an interoperable, extensible, real-time routing protocol for the movement of mission-critical information, such as instant messages, presence and structured data between previously non-interoperable systems."[561]

The ISE also relies heavily on the creation of electronic directories, which is made possible through private sector research and development. As emphasized by the ISE Implementation Plan, the creation of electronic directories is often a government department or agency's first step toward improving information sharing with other ISE partners. Kevin McCook, director of federal sales for Verity Inc., has argued that "EDS [electronic directory services] is essential plumbing"[562] for information sharing initiatives. "It has to be there for the rest of the ISE to work," he claimed. Since September 2005, the federal government has tapped into the expertise of private sector entities to develop improved means for ISE participants to locate and communicate with others. Private sector experts

557 *FBI Announces, supra* note 470.
558 *AEP Networks Exhibit at All Hazards Forum Showcases Homeland Security Solutions*, Market Wire, Oct. 24, 2005.
559 *Ibid.*
560 *General Dynamics and Jabber, Inc. Partner to Facilitate Information Sharing and Systems Interoperability*, Business Wire, Sept. 20, 2005.
561 *Ibid.*
562 Miller, *supra* note 61.

are currently working to build upon existing technology and provide EDS for more complex, larger scale information sharing environments.[563]

Companies of interest to ISE participants also include Lockheed Martin, which has recently acquired The Sytex Group, ChoicePoint, which specializes in the development of large-scale data networks, and LexisNexis, which has purchased Seisint, Inc. and provided information technology to the CIA.[564]

Non-Profit Sector Involvement: The Markle Foundation

The John and Mary R. Markle Foundation, Inc. finds creative uses for information and information technology in addressing critical public needs. Founded in 1927, the Foundation's general mission is "to promote the advancement and diffusion of knowledge...and the general good of mankind."[565] From initial work in traditional social welfare and medical research projects, the Foundation's focus shifted in the 1960s to mass communications and information technology, which has since dominated the Foundation's programming.

When Zoë Baird became Markle's president in 1998, the Foundation began researching ways in which communications could facilitate the resolution of complex issues, empower people, and serve public needs. These efforts prompted the Foundation to develop a roundtable problem-solving approach that brings together leaders from the fields of technology, business, and government. The Foundation's determination to collaborate with public and private sector experts enables it to have a broader impact on the development of public policies in areas where information technology plays a critical role. Recently, the Markle Foundation has concentrated on modernizing healthcare and strengthening national security and terrorism prevention.[566] In both of these areas, the Foundation has demonstrated a commitment to safeguarding privacy and civil liberties.[567]

The Foundation's work on the intersection of information technology and counter-terrorism policy has been carried out by the Markle Task Force on National Security in the Information Age. Established in April 2002, Task Force members have included national security policymakers of the Carter, Reagan, Bush and Clinton administrations, as well as senior executives from the information technology industry, civil liberties advocates, lawyers, and intelligence experts.[568] The purpose of the Task Force has been to advise federal, state and local governments as they develop policy on the collection, use, and sharing of terrorism information. By proposing ways to enhance America's security while protecting civil liberties, the Task Force has shaped the strategies and legal issues that inform ISE implementation.

Research Contributions

Since its inception, Markle's Task Force on National Security in the Information Age has released three reports on establishing an information sharing environment. The Task Force's research contains careful reviews of the nation's current national security infrastructure and makes recommendations on leveraging technology for improved information sharing while protecting civil liberties.

Not long after the 9/11 attacks, the Task Force emerged as a strong voice advocating the use of information policy and technology to improve counter-terrorism efforts. Its 2002 report, *Protecting America's Freedom in the Information Age*, provided strategies on harmonizing the domestic

563 *Ibid.*

564 *The Private Sector's Role, supra* note 532.

565 Markle.org, Markle Foundation, Foundation History, http://www.markle.org/about_markle/foundation_history/index.php (last visited Jan. 27, 2008).

566 *Ibid.*

567 *Ibid.*

568 Markle.org, National Security, Markle Foundation, http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/index.php (last visited Jan. 27, 2008).

security functions of DHS and the FBI while also advancing the Task Force's position that "information analysis is the brain of homeland security."[569] In the report, the Task Force argued that the newly created Department of Homeland Security should be a "hub" for information policy decision-making. The Task Force urged that DHS' responsibilities include improving data collection and analysis procedures and shaping information sharing initiatives. The report also recommended that DHS "take the lead" in developing guidelines to protect privacy and civil liberties, which "should harness "authentication, certification, verification, and encryption technologies."[570]

This first report elaborated on civil liberties concerns by suggesting that information handling accountability policies, audits, and carefully designed rules on the retention and dissemination of personally identifiable information be created. The Task Force also called for strong presidential leadership of efforts to protect privacy: "Only the President can establish and be accountable for the proper balance between development of domestic intelligence and preservation of liberty."[571]

Recognizing the value of terrorism information collected by SLT entities and law enforcement officers in the field, *Protecting America's Freedom in the Information Age* advocated a decentralized approach to information sharing, a key recommendation that has since guided the architecture of the ISE. The report recommended the development of multi-level government sharing networks, which should be designed "from the bottom up" to meet the needs of local participants. If "implemented with the simplest design possible," these networks could be easily updated as policies and technology change to meet evolving threats. The report also argued that vertical information sharing should be strengthened by efforts to "empower local participants" and enable local experts to contribute their expertise at the "edge" of sharing networks. The Task Force flagged allocation of funding and the availability of training as crucial to changing "need to know" mentalities, upgrading technological capabilities, and enhancing human analysis skills.[572]

Finally, the Task Force's initial report offered suggestions on improving information analysis. Noting that "intelligence is often conceived as perpetrator-centered and event focused," the Task Force recommended that DHS strengthen its "peripheral vision" by identifying "valuable potential *targets*" and "the most dangerous *means* that could be used to attack them." Such "wide scans" for vulnerabilities would enhance risk and threat management and optimize the value of real-time information exchange.[573]

In 2003, the Task Force built upon previous information sharing recommendations with the release of its second report, *Creating a Trusted Information Network for Homeland Security*. The report renewed many of the recommendations set forth in *Protecting America's Freedom in the Information Age* and provided more detailed strategies on adopting a decentralized network approach to information sharing. The report praised the government's greater willingness to advance a "need to share" culture but also lamented the absence of a national strategy for improved information sharing and noted that between 2002 and 2003, "progress…[had] been ad hoc and sporadic at best."[574] To provide a more concrete model for horizontal and vertical information sharing, the Task Force proposed that the government implement its vision of the Systemwide Homeland

569 The Markle Foundation Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age*, *available at* http://www.markle.org/downloadable_assets/nstf_full.pdf.
570 *Ibid*.
571 *Ibid*.
572 *Ibid*.
573 *Ibid*.
574 The Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security*, *available at* http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf.

Analysis and Resource Exchange (SHARE) Network.

As described by the Task Force, the SHARE Network would link federal, SLT, and private sector entities to an information sharing system that does not depend upon any centralized databases and therefore would have "no single points of failure." The network would offer a "decentralized, peer-to-peer environment" through which information sharing could occur across "multiple and redundant communication pathways." The system would be flexible, upgradeable, and able to accommodate both routine and ad hoc information sharing. In the Task Force's envisioned system, users could identify and locate participating persons through complex EDS capabilities. The network would also host real-time communications while securing information through access control, encryption, and electronic audit mechanisms.[575]

In addition to outlining the capabilities of its communications model, the Task Force's second report also offered recommendations on how the SHARE Network could be implemented. The report devoted considerable discussion to the roles and responsibilities of key federal actors and argued that strong leadership, clear objectives, and the development of processes to assess agencies' progress would be critical to the success of such a network. To provide a concrete "action plan," the Task Force proposed the contents of two hypothetical Executive Orders, which would delineate privacy guidelines and designate DHS as the "lead agency" for interagency sharing initiatives. As part of its "action plan," the Task Force also recommended that the FBI work directly with state and local law enforcement agencies to develop data sharing policies that protect privacy and ensure robust participation in the proposed network. Finally, the Task Force urged that Congress fulfill an essential oversight role by reviewing federal performance, evaluating privacy policies, and examining the extent to which SLT and the private sector entities are integrated into the sharing network.[576]

By 2006, the Task Force recognized that many of its recommendations regarding the SHARE Network had not been implemented and that critical ISE participants were still "stovepiping" information. The Task Force commented, "We have witnessed some genuine improvements in information sharing…[but] two years since the publication of our last report, and almost five years since the terrorist attacks of September 11, systematic, trusted information sharing remains more of an aspiration than a reality."[577] This observation provided the impetus for the release of the Task Force's third report, entitled, *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*. This publication "call[ed] for a renewed commitment by our nation's leaders to the development of an information sharing environment" and set forth proposals to accelerate ISE implementation.[578]

Whereas the Task Force's earlier reports concentrated on key organizational and technical issues, *Mobilizing Information to Prevent Terrorism* emphasized the need to overcome cultural and bureaucratic barriers to information sharing. The Task Force asserted that improved accountability and coordination policies, as well as increased training opportunities, are needed to facilitate a collaborative working environment among ISE participants. The report also promoted a "risk management approach" to classified information sharing that would help deconstruct remaining "need to know" policies. This approach would require officials to make information handling decisions by "balanc[ing] the risks of disclosure with

575 *Ibid.*

576 *Ibid.*

577 The Markle Foundation Task Force on National Security in the Information Age, *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, *available at* http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf [hereinafter Markle, *Mobilizing Information*].

578 *Ibid.*

the risks of failing to share information." The Task Force's recommendations on closing cultural gaps also included a suggestion on establishing a new Information Sharing Institute. The Institute, consisting of public and private sector experts, would provide materials on best practices and further investment in the research and development of information sharing technology.[579]

In addition to addressing cultural barriers to sharing, the Task Force's third report highlighted key trust issues, which spanned the following topics: (1) the need for ISE participants to build trustful relationships that support information sharing; (2) the need for policymakers to trust that the legal framework of the ISE is "being implemented, followed, and enforced in good faith;" and (3) the need for the public's trust that the ISE is being implemented with appropriate regard to privacy and civil liberties values. The Task Force claimed that persistent leadership; healthy oversight from the executive, legislative, and judicial branches of government; transparent sharing policies; and the use of technology that includes privacy mechanisms, are all crucial to effective trust-building.[580]

On civil liberties protection, the Task Force's third report advocated the development of an "authorized use" standard for sharing classified information. Task Force member Jim Dempsey, who is also policy director of the Global Internet Policy Initiative at the Center for Democracy and Technology, remarked, "The borderless nature of the threat has rendered unworkable some of the old rules on sharing lawfully collected information."[581] The Task Force's proposed method would therefore base information access decisions on the use to which the information will be put and ISE participants' specific missions, rather than on users' nationality or the place of the information's collection.[582] Dempsey added, "Under the authorized use approach we propose, each agency can get the information it needs to pursue a clearly articulated mission, subject to auditing to ensure accountability and protect privacy."[583] The Task Force instructed that principles guiding the development of an "authorized use" standard should be developed through "open public debate."[584]

The Markle Foundation's Task Force on National Security in the Information Age has not met since the release of its third publication in 2006. Task Force members have claimed that they wish to provide the government with needed time to implement the recommendations contained in their publications.[585] Dempsey has also stated that the body halted its work because too frequent issuance of recommendations and criticism could inadvertently jeopardize the Task Force's goal of advancing needed policy change.[586] There remains the possibility that the Task Force will reconvene in the near future to assess and guide the administration's information sharing initiatives.

Assessing the Markle Foundation's Impact on ISE Implementation

The Markle Foundation's Task Force on National Security in the Information Age has emerged as one of the most vocal expert bodies on information sharing issues and has been credited with a considerably influential role on national security policymaking. The Task Force's recommendations have resulted in tangible legal and policy shifts, though some critics assert that the Task Force's impacts on policy are often overstated.

579 *Ibid.*
580 *Ibid.*
581 *Markle Task Force on National Security in the Information Age Releases Third Report*, Business Wire, July 13, 2006 [hereinafter *Markle Task Force Release*].
582 Markle, *Mobilizing Information, supra* note 577.
583 *Markle Task Force Release, supra* note 581.
584 *Ibid.*
585 Michael Arnone, *IT For the Common Good*, Gov't Health IT, *available at* http://govhealthit.com/article95712-08-21-06-Print&printLayout [hereinafter Arnone].
586 *Ibid.*

The quality of the Task Force's reports and the content of its recommendations reflect careful consideration of relevant law and policy, as well as strategic and technical issues. The Task Force's methodology has been met with praise from non-profit and private sector entities.[587] Thomas Marsden, assistant vice president of Dun and Bradstreet's Government Solutions, has commented that the Task Force's extensive research enables its members to pinpoint clear, specific, and reachable information sharing objectives.[588]

The Task Force's careful work has resulted in Congress's decision to embody many of its recommendations in the provisions of the IRTPA. Senators Joseph Lieberman and Susan Collins, in debating the IRTPA's contents, advanced the Task Force's proposals on policies protecting civil liberties and argued for the Task Force's conception of the "attributes" of a "trusted information sharing environment."[589] The Task Force's work has also achieved greater awareness of information issues and their importance. Along with the 9/11 Commission Report, the Task Force's 2002 and 2003 reports permitted policymakers and members of the public to develop a better understanding of the way in which inadequate information sharing policies hindered the nation's ability to detect, prevent, and respond to the 9/11 attacks. The Markle Foundation's impressive reputation on analyzing civil liberties issues has likewise highlighted privacy concerns that continue to challenge ISE implementation.

However, some critics contend that the Markle Foundation has concentrated far less on privacy and civil liberties issues in the national security context than in its other research areas. Though the Task Force proposed the adoption of the "authorized use" standard and technologies featuring electronic audit mechanisms in its third report, critics claim that the Task Force's recommendations on protecting privacy are far less concrete or extensive than its recommendations on the increased collection, retention, and flow of data.[590] American Civil Liberties Union (ACLU) attorney Timothy Sparapani has argued that members of the Task Force "say all the right stuff" but that their discussion of privacy issues ultimately lack substance.[591] Similar accusations by other civil libertarians have raised some questions as to the extent of the Markle Foundation's commitment to privacy and civil liberties issues in the national security arena.[592]

Others have pointed out that despite Congress' adoption of several of the Markle Foundation's recommendations, the Task Force's impact on the development of the ISE has been limited. For example, Jim Harper, director of information policy studies at the Cato Institute, has criticized the Markle Foundation as "wonderfully self-congratulatory" in assessing its own influence on the development of the ISE.[593] While advancing information sharing, the Bush administration has maintained a distance from the Task Force's insistence that its particular vision of the SHARE Network be implemented.[594] After all, the fact that an insufficient number of its recommendations had been implemented was admittedly one of the Task Force's reasons for issuing its third report.[595]

Though the Markle Foundation's direct influence on policymakers is debatable, the non-profit organization has certainly offered a valuable contribution to ISE implementation by gathering experts from diverse backgrounds to analyze the most challenging information sharing issues. When still convening, the Task Force's members consisted of representatives from government, academia, the information technology industry, law firms, and policy think tanks. Though Sparapani

587 *Ibid*.
588 *Ibid*.
589 *Privacy of Health Records*, CQ Congressional Testimony, Feb. 1, 2007.
590 Arnone, *supra* note 585.
591 *Ibid*.
592 *Ibid*.
593 *Ibid*.
594 *Ibid*.
595 Markle, *Mobilizing Information, supra* note 577.

critiqued some of the Task Force's recommendations regarding civil liberties, he acknowledged that the Markle Foundation "brings the focus of serious people to bear on pressing problems."[596] The Foundation's work has refined the public discourse on homeland security issues and fostered a greater understanding of the urgency with which policymakers should implement the ISE.

III. Future of the ISE: Conclusions and Preliminary Recommendations

Continuing foreign and domestic terrorist threats to the United States makes it essential to continue national efforts to create an information sharing environment among federal, SLT, foreign, and private sector actors. Considerable progress has been made in this regard since 9/11. Nevertheless, substantial legal, policy, technical, and cultural impediments remain.

Under its first program manager, John Russack, the ISE had struggled to launch large-scale sharing efforts. Russack frequently complained that his office was understaffed and that Congress had failed to allocate sufficient funds for him to effectively carry out his duties.[597] Russack determined that his office required $30 million "as a minimum" for launching a sustained information sharing effort, but he had received only $9.6 million in FY 2005.[598] His resignation in January 2006 presented a considerable impediment for timely achievement of the goals set forth in the IRTPA, leaving members of Congress very concerned.

Despite having to overcome this legacy of a slow start, Russack's successor as Program Manager, Ambassador Ted McNamara, has enjoyed certain advantages. For example, Enhanced awareness of the necessity for improved sharing, promoted by both the *9/11 Commission Report* and the Markle Foundation's publications, has enabled ISE policies to occupy the foreground of homeland security debates. As ISE implementation has progressed, policymakers have demonstrated a deeper commitment to the incremental transformation of "need to know" policies into a "need to share" culture that favors decentralized information collection and robust dissemination practices.

On a strategic level, enactment of the IRTPA has greatly improved upon sharing initiatives launched by the USA PATRIOT Act and the Homeland Security Act of 2002. By providing clearer sharing objectives and calling for needed presidential guidance, the IRTPA defined the ISE and established a framework for managing the structural changes of evolving information sharing practices. The legislation also provided needed institutions, such as the Privacy and Civil Liberties Oversight Board, for safeguarding legal rights.

Though its release had been delayed, the ISE Implementation Plan (Plan) also offers essential guidance for expanding collaborative information sharing strategies. The Plan carefully delineates the roles and responsibilities of participants in implementing horizontal and vertical sharing practices and sets an aggressive, but reachable, timetable ending in 2009. MacKenzie Eaglen, a policy analyst at the Heritage Foundation, has remarked that "coordinated strategies," such as those contained in the Plan, offer "sound policies,"[599] rather than initiatives that simply encourage the development of technology "in a vacuum."[600] As challenges to information sharing tend to be more cultural than technical, the strategies and goals set forth in the Plan provide an important framework for enabling ISE participants to achieve greater cooperation and therefore optimize the value of emerging technologies.

Recent initiatives have also resulted in tangible information sharing improvements. The law en-

596 Arnone, *supra* note 585.
597 Yoest, *supra* note 27.
598 *Ibid.*
599 *Security; Federal Information-Sharing Plan May Face Hurdles*, Technology Daily, Nov. 29, 2006.
600 *Ibid.*

forcement community's expansion of the JTTFs, use of the RISS and N-DEx networks, and development of consolidated terrorism databases at the TSC have strengthened interagency partnerships. The DoD's information technology upgrades and ongoing efforts to incorporate foreign actors into the ISE have also yielded tangible results in military operations. The DHS, while facing numerous challenges in implementing the HSIN, has contributed to vertical information sharing and multi-jurisdictional relationship building through increased collaboration with state and local fusion centers. Though the intelligence community continues to struggle with the information classification system, DNI CIO Meyerrose has affirmed that intelligence officials have greater access to information collected by other agencies. "Large volumes of information," he stated, are now often accessible to intelligence analysts "at the stroke of a keyboard."[601]

These successes must stimulate ISE participants to vigorously tackle remaining challenges. One of the most urgent issues involves the status of HSIN. Haphazard implementation and reliance on a "top down" approach has severely prevented the network from meeting the needs of its SLT users. DHS must redouble its efforts if HSIN is to perform its intended role as the primary mechanism for vertical information sharing. Where sharing has generally been more successful, such as on the horizontal level, bureaucratic processes and resistance to change have allowed "need to know" policies to persist in a variety of contexts. This cultural hurdle illustrates that while the government depends upon effective information technology in implementing the ISE, improved sharing cannot be purchased.[602] Rather, technological capabilities will prove useful only when combined with strong leadership, clear goals, and insightful strategies. As the 9/11 Commission cautioned in its Report, "even the best information technology will not improve information sharing so long as…agencies' personnel and security systems reward protecting information rather than disseminating it."[603]

Federal authorities must accelerate security clearance reforms and ISE implementation procedures if the ISE is to fully integrate SLT and private sector partners by the Implementation Plan's 2009 deadline. GAO and DHS IG reports of sluggish and cumbersome information sharing initiatives, though frustrating, must serve to invigorate sharing initiatives. Six years after 9/11, the federal government has succeeded in identifying many gaps in information sharing but has been only partially able to resolve them.

The following preliminary recommendations aim to strengthen the ongoing implementation of the ISE. As time progresses, the President, Congress, PM-ISE, and heads of relevant departments and agencies bear the responsibility of ensuring that ISE participants remain focused on the need to overcome remaining information sharing challenges. Establishing a multi-jurisdictional information sharing environment is a difficult, but reachable, goal. The nation's ability to protect itself from terror and other security threats will depend upon the effectiveness of leadership and oversight provided by all three branches of government, as well as ISE participants' commitment to developing more robust communications.

Preliminary Recommendations

• Federal and SLT departments should offer improved information sharing training opportunities for their workforces.

A review of ISE implementation efforts across participating communities indicates that, while numerous sharing initiatives have been launched, some with considerable success, sharing has not

601 Shaun Waterman, *Report Slams U.S. Terror Info Sharing*, UPI, Apr. 18, 2006.

602 Michael Bruno, *Info-Sharing Solutions Sought, Homeland Defense Commander Says*, Aerospace Daily & Defense Report, Feb. 24, 2005.

603 National Commission of Terrorist Attacks, *supra* note 1.

yet become an integral element of these communities' daily operations. Training opportunities should educate workforces on how to integrate emerging technology and altered information handling policies more effectively into routine procedures. Interagency training exercises can also foster a cooperative atmosphere and provide trust and relationship-building opportunities, elements that encourage information sharing.

• Agencies must engage in a collaborative effort, guided by the Office of the Program Manager and the ISC, to develop clearer quality-control policies for shared information.

Examining the sheer quantity of shared information does not provide an accurate measure of the ISE's success. Rather, shared information must be filtered to avoid duplication and ensure that information is provided in a form most valuable to receiving parties. Officials across the ISE's participating communities have complained that, at least occasionally, their agencies have been overwhelmed by the "volume, velocity and variety" of information transmitted to them. One senior intelligence official, for example, referred to shared information as a "tidal wave" and claimed, "We can either be drowned by it or we can get on our surfboard and surf it and let it propel us."[604] To ensure that ISE participants remain "on the surfboard," departments and agencies must establish clearer policies on the processing and filtering of the data to be shared through the ISE.

• The DHS must urgently develop policies to improve the sharing capabilities of the HSIN.

The HSIN was intended to link homeland security, fusion center, intelligence, and law enforcement officials in a comprehensive, decentralized network. Because of the network's current failure to provide a central artery for homeland security communications, its intended users have turned toward ad hoc, and often inefficient, means for obtaining needed information. Unchanged, this situation could lead to the "stovepiping" of information in compartmentalized, limited-access databases and thwart the development of trusted partnerships necessary for successful information sharing. Steps toward improving the HSIN should include the adoption of a "bottom up" approach that carefully considers the needs of SLT users and filters duplicative HSIN. The DHS must also prioritize efforts to accelerate security clearance procedures so that classified information needed by fusion center and SLT officials may be integrated into HSIN.

• The ISE should offer first responders greater access to information sharing portals.

Senator Lieberman has asserted: "9/11 showed that it is imperative in a disaster for first responders to be able to talk to each other. It's clear that many of the first responders died on 9/11 in New York because they couldn't communicate with one another. Hurricane Katrina showed us four years later that we still have a long way to go."[605] Many current policies tend to assume that SLT and law enforcement officials will disseminate needed information to first responders. However, the critical role of first responders in mitigating the effects of a terrorist attack warrant their increased participation in the ISE. First responders must have a clear understanding of how to access and transmit information to both SLT and federal entities in the event of a homeland security incident.

• In addition to establishing accountability and audit policies, ISE participants should engage in simulations to test the progress of information sharing initiatives and identify remaining vulnerabilities.

While ISE implementation has already improved departments and agencies' situational awareness,

604 *The Private Sector, supra* note 532.

605 *Ensuring Full Implementation, supra* note 74. *See also* Richard Weitz, *Enhancing Emergency Communications Interoperability*, WASH. POST, Feb. 16, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/02/15/AR2007021500816.html.

ISE participants should carry out simulations to enhance their ability to share information in an emergency. Simulation exercises offer ISE participants an opportunity to refine coordination and communications capabilities in highly complex hypothetical scenarios. Simulations serve as important tools for assessing the effectiveness of information sharing strategies and preparing ISE participants for managing the effects of both natural disasters and terrorist attacks.

• The Office of the Program Manager should develop clearer guidelines for facilitating vertical information sharing.

Many SLT partners have complained that, despite collaboration with federal officials at fusion centers, they are generally uncertain about which information should be shared and how the data sharing should occur. If a local law enforcement official observes suspicious activity in the field, he or she needs clear guidelines to: (1) assess whether that information should be reported to federal and/or SLT participants in the ISE; (2) unambiguously determine which agencies must receive information that he or she decides warrants reporting; and (3) easily locate a point of contact through efficient electronic directory services.

• The Office of the Program Manager should promote greater public awareness of the ISE as well as informed discussion of information sharing and privacy initiatives.

Smooth functioning of the democratic process represents an essential element of the ISE's success in protecting privacy and civil liberties. Transparent information sharing practices will improve the public's ability to influence policymakers' decisions on security and privacy needs. Transparency also cultivates public trust in new security measures and ensures that public debate of information sharing issues consists of informed discussion. Unlike the aftermath of Poindexter's Total Information Awareness (TIA), public deliberations of ISE policies should reflect careful consideration of relevant issues, rather than fear or hype. An informed public discourse will improve Congress' ability to provide appropriate oversight for information sharing activities and assess the risks and benefits of emerging technological capabilities, such as data mining.

• Congress should consider the Markle Foundation's recommendation of establishing an Information Sharing Institute.

According to the Foundation's proposal, an Information Sharing Institute could minimize gaps in federal, SLT, and private sector data exchange by developing and improving sharing strategies. The Institute would also enhance the efficiency of sharing procedures by analyzing and compiling information on best practices. Similar to nonprofit policy organizations or think tanks, the Institute would provide recommendations of experts representing a variety of backgrounds, including government, industry, information technology, policy, and law.

5.2 Preventing the Poisoning of the Well: A Consideration of the Necessity and Legality of Broadening the Protection of Critical Infrastructure Information in the Interest of National Security and Public Safety

by Paul D. Barkhurst, Jr., J.D.[606]

Introduction

In the U.S. Air Force, when you receive a "Frag" (literally a"fragment" of the Air Tasking Order) of that evening's target, your first task is to gather all available information on the target so as to figure out the best way to blow it up. This would entail maps, diagrams, photographs, or anything else

606 The author is a former USAF aviator and JAG who processed FOIA Appeals for the Secretary of the Air Force and defended FOIA cases against the USAF in federal court. He currently represents local governmental entities in condemnation and construction litigation.

that would show the vulnerability of the target. Some aircraft, such as the venerable F-111, the F-117, and the F-15E, fly an air-to ground mission known as "air interdiction," which often means the destruction of the enemy's public infrastructure which exists well beyond the battlefield and deep inside enemy territory.[607] Interdiction has been defined as "an attack against the source of men and material."[608] In Desert Storm, for example, many power plants, telecommunications systems, bridges, highway intersections, factories, etc. were targeted by these aircraft using laser-guided bombs ("LGBs").[609]

The idea behind strategic interdiction is that if you destroy enough of a country's ability to function, transport, travel, communicate, etc., you can undermine the war fighters and destroy the enemy nation's will to fight. Terrorists think in much the same way, but they do not have (a) a legitimate declaration of war under Article 51 of the Charter of the United Nations[610], or (b) the luxury of multi-million dollar fighter attack jets. Of course, as we witnessed on September 11, 2001, they nevertheless mounted a successful aerial attack against some of our critical economic and military infrastructure using flying bombs that were intended to be commercial passenger jets.

Continuing with this analogy, then, if one was the mastermind of a terrorist cell, and one was tasked with killing as many Americans as possible by, for example, poisoning the water supply, blowing up a nuclear power station, or gassing a subway system's air ventilation system, then one would want, as a starting point, the designs and plans for these items of critical infrastructure. In the U.S. military, such documents, as they relate to an enemy's infrastructure, are classified typically as "Top Secret" documents.[611] This begs the question of why we as a nation, a state, or a city would want to simply hand over those plans to those who wish to destroy our critical infrastructure.

"Critical Infrastructure"

It is not hard to imagine what we should term "critical infrastructure" when all we need to do is look at the targets which terrorists have historically chosen to attack: public buildings, airports, airplanes, trains, subway systems, nuclear power stations, water supply systems, etc. The legal definition of "critical infrastructure" is contained in the Critical Infrastructure Protection Act of 2001 ("CIPA").[612] The CIPA defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[613]

Furthermore, the Office of Infrastructure Protection ("OIP") of the Department of Homeland Security ("DHS") has a list of some 77,000 assets in the National Asset Database[614] that it considers important enough to consider protecting, in the interest of national security, and public health and safety.

Constitutional Implications of Protecting Information

This Paper is not intended to be an examination of whether our government should protect critical infrastructure information, but whether it can. This study will be made not just under the existing

607 *See generally* John A. Warden, III, *The Air Campaign: Planning for Combat*, National Defense University Press, 1988.
608 *See id.*
609 *Conduct of the Persian Gulf War: Final Report to Congress*, U.S. Dept. of Defense, 3 vol. The Air Campaign, v. 1, pp 113-247 (1991).
610 June 26, 1945, T.S. No. 993.
611 *See* Exec. Order No. 12,356, 47 Fed. Reg. 14874 (Apr. 6, 1982).
612 42 U.S.C. § 5195c (2001).
613 *See id.*
614 *See* John Moteff, CRS Report for Congress, *Critical Infrastructure: The National Asset Database* (Updated July 16, 2007).

laws, but will delve into potential future legislation. At the center of this endeavor is the proper balance between open government and national security. Where and how to draw these lines is a continual debate, with the pendulum swinging towards increased protection as the threat of further terrorist attacks on U.S. soil increases.

As James Madison said, "A popular government without popular information or the means of acquiring it, is but a Prologue to Farce, or a Tragedy, or perhaps both. Knowledge will forever govern ignorance, and a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."[615] However, this statement was made in a time and in a context where Americans had only recently won freedom from tyranny and an oppressive imperial government which refused to afford its far flung colonies even the most basic of inalienable rights. In a technological environment that allows instant information access from cyber space and instant death from nuclear, biological, and chemical weapons, the potential effects of terrorist activity are more disastrous then ever before. As a result, the protection of information has never been so important. As Chief Justice Rehnquist stated, "In any civilized society, the most important task is achieving a proper balance between freedom and order. In wartime, reason and history suggest that this balance shifts to some degree in favor of order – in favor of the government's ability to deal with conditions that threaten the national well being."[616] This statement seems more fitting for the modern United States than the words of James Madison. Finally, it must not be forgotten that while the freedoms of speech, religion, and assembly are guaranteed by the U.S. Constitution, freedom of information is a creature of statutory creation which can expand and contract based on the needs of the time. And these indeed are troubled times.

615 James Madison, August 4, 1822.

616 Chief Justice William Rehnquist, All the Laws But One: Civil Liberties in Wartime (New York: Knopf, 1998), p. 222.

The Freedom of Information Act and its Exemptions

The federal government and all fifty states have some sort of open records legislation on the books, of varying degree and quality.[617] Most of these are modeled after the federal Freedom of Information Act of 1966[618] ("FOIA") which was passed in response to public outcry against government secrecy spawned by the Cold War, and public mistrust caused by the Vietnam War.[619] The FOIA has an initial presumption of disclosure, but contains nine discrete exemptions based on a careful balancing of the harm of disclosure with the public's right to know.[620] Of the nine enumerated exemptions, there are four which appear at first blush to be viable candidates for the protection of critical infrastructure information: Exemption 1 (classified information in the interest of national security), Exemption 2 (internal agency procedures), Exemption 3 (exempted by statute), and Exemption 4 (confidential business information).

FOIA Exemption 1 exempts matters of national security from disclosure such as classified military information, pursuant to Executive Order of the President.[621] It would be difficult for anyone to argue that making information about military weapons, tactics and operations freely available to the world would be a good thing. Indeed, the courts have historically allowed the various federal agencies, particularly the Department of Defense, the Department of State, and the Department of Justice, considerable deference in the classification of documents in the interest of national security. In EPA v. Mink,[622] the Supreme Court held that records which were classified pursuant to proper

617 *See generally* 37A Am. Jur. 2d *Freedom of Information Acts* § 2, "State Freedom of Information Acts" (2007).

618 5 U.S.C. § 552.

619 Robert L. Saloschin, *The Department of Justice and the Explosion of Freedom of Information Act Litigation*, 52 Admin. L. Rev. 1401, 1407. (2000).

620 *See* 5 U.S.C. § 552(b).

621 *See* Exec. Order No. 12,958.

622 410 U.S. 73 (1973).

procedures were per se exempt from disclosure, without further review by the courts. Congress reacted in 1974 with an amendment which expressly provided for de novo review by the courts, and for in camera review of classified documents, where appropriate.[623] As a result, the practice developed whereby the federal agencies would file an affidavit and a summary judgment based on agency discretion, and this practice has largely been upheld by the courts.[624]

However, when one reviews this case law regarding Exemption 1, and sees the substantial judicial deference that has largely gone into upholding such agency determinations, one realizes that critical infrastructure, while important to national security, does not rise to the level of Exemption 1 protection, and trying to pigeon-hole it here would only muddy the water of some otherwise crystalline case law.

Exemption 2, likewise, does not initially appear to be a good place to put the protection of critical infrastructure as the exemption applies to information "related solely to the internal personnel rules and practices of an agency."[625] However, Exemption 2 applies to more than just trivial internal matters such as routine personnel policies, leave procedures, etc. (known as "Low 2" information). It also applies to more substantial internal matters, the disclosure of which could risk the circumvention of a statute or agency regulation; e.g. law enforcement manuals.[626]

In 1981, the D.C. Circuit, which has become the preeminent court in FOIA litigation through the sheer volume of its FOIA decisions, handed down the seminal "High 2" category case of Crooker v. ATF.[627] The Crooker Court, in holding that the ATF's training manual was exempt from disclosure under Exemption 2, held that, to be protected under the "High 2" exemption, a document should be "predominantly internal", and that its disclosure "significantly risks circumvention of agency regulations or statutes."[628] Indeed, the DOJ's Office of Information and Privacy ("OIP") issued a memo in 2001 which encourages agencies to use Exemption 2 to protect critical infrastructure information: "Agencies should be sure to avail themselves of the full measure of Exemption 2's protection for their critical infrastructure information as they continue to gather more of it, and assess its heightened sensitivity, in the wake of the September 11 terrorist attacks."[629]

However, the problems with Exemption 2 are: (1) most of the nation's critical infrastructure is held in private ownership; e.g., AT&T;[630] or (2) is held by state and local governments; e.g., Three Mile Island Unit 2 nuclear power plant; and (3) Exemption 2 patently applies to the internal records of federal agencies. Thus, since most of the nation's critical infrastructure is held by private enterprise, the next most logical place to seek protection from disclosure would be Exemption 4.

FOIA Exemption 4 protects information that is comprised of "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[631] The vast majority of the documents protected by Exemption 4 are referred to as "confidential business information". In the watershed case of National Parks & Con-

623 5 U.S.C. § 552(a)(4)(B).

624 *See* Halperin v. CIA, 629 F.2d 144, 148 (D.C. Cir. 1980) (noting that judges "lack the expertise necessary to second guess such agency opinions in the typical national security case").

625 5 U.S.C. § 552(b)(2).

626 *See*, e.g., Department of the Air Force v. Rose, 425 U.S. 352, 364 (1976) (recognizing the category but expressly leaving open the question of Exemption 2's applicability).

627 670 F.2d 1051 (D.C. Cir. 1981) (en banc).

628 *Id.* at 1073-74.

629 *See* OIP, New Attorney General FOIA Memorandum Issued, posted Oct. 15, 2001, available at www.usdoj.gov/ oip/foiapost/2001foiapost19.htm.

630 "The private sector … owns and operates the vast majority of America's critical infrastructure." Remarks of HAS Director Thomas Ridge, Oct. 9, 2001, available at www.whitehouse.gov/news/releases/2001/10.

631 5 U.S.C. § 552(b)(4).

servation Association v. Morton,[632] the D.C. Circuit held that commercial business information is protected if its release would either: "(1)…impair the Government's ability to obtain necessary information in the future; or (2)…cause substantial harm to the competitive position of the person from whom the information was obtained."[633] In 1992, the D.C. Circuit further fleshed out this standard in the case of Critical Mass Energy Project v. NRC.[634] The Critical Mass Court held that the threshold matter to be determined is whether the information was submitted to the government "voluntarily," and if so, then the information is protected, provided that it is not "customarily" disclosed to the public by the private party.[635]

It is clear that Exemption 4 protects a greater class of critical infrastructure information that Exemption 2; however, it still does not go far enough for two reasons. First, Exemption 4 does not protect information which a private critical infrastructure owner chooses not to voluntarily share with the federal government; i.e., because they do not want to risk the disclosure of their confidential, proprietary trade secret information. Second, much of critical infrastructure is owned and operated by state and local governments, and this too is not covered by Exemption 4. This leads us to a consideration of Exemption 3.

FOIA Exemption 3 protects information "specifically exempted from disclosure by statute…provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld."[636] Broadly speaking, Exemption 3 of the FOIA incorporates the prohibitions against disclosure which are contained in various other federal statutes. As originally passed into law, the provision simply exempted from disclosure all information which other federal statutes sought to protect. Indeed, the high watermark for this exemption was expressed by the Supreme Court, in FAA v. Robertson[637], wherein the Court held that statutes enacted prior to the FOIA, which gave broad withholding power to various federal agencies, were largely unaffected by the disclosure mandate of the FOIA. Congress responded in 1976 by amending Exemption 3 to allow withholding of information under Exemption 3 only if one of two specific criteria are met; i.e., if the withholding statute "(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld."[638] With these criteria in mind, we turn now to Congress' efforts to protect critical infrastructure laws fashioned to fit into Exemption 3's exacting criteria.

The Critical Infrastructure Protection Act of 2001 and the Critical Infrastructure Information Act of 2002

Effective October 26, 2001, Congress passed the Critical Infrastructure Protection Act ("CIPA"),[639] which defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[640]

With the Critical Infrastructure Information Act of 2002 ("CIIA"),[641] Congress brought information relating to "critical infrastructure" under the umbrella of FOIA Exemption 3 protection. The CIIA provides, in pertinent part:

632 498 F.2d 765 (D.C. Cir. 1974).
633 *See id*. at 770.
634 975 F.2d 871 (D.C. Cir. 1992) (en banc).
635 *Id*. at 878.
636 5 U.S.C. § 552(b)(3).
637 422 U.S. 255, 266 (1975).
638 5 U.S.C. § 552(b)(3).
639 42 U.S.C. § 5195c.
640 *Id*.
641 6 U.S.C. § 131, et seq. (Amended July 7, 2004).

> Notwithstanding any other provision of law, critical infrastructure information … that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—
> (A) shall be exempt from disclosure under section 552 of Title 5 (commonly referred to as the Freedom of Information Act);
> (B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;
> (C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;
> (D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this part, except--
> (i) in furtherance of an investigation or the prosecution of a criminal act; or
> (ii) when disclosure of the information would be--
> (I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or
> (II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office. [FN1]
> (E) shall not, if provided to a State or local government or government agency--
> (i) be made available pursuant to any State or local law requiring disclosure of information or records;
> (ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or
> (iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act…[642]

The intent of the above language is very clear; i.e., that broad categories of information related to critical infrastructure are considered non-releasable to the general public in the interest of national security. The "voluntary" provision appears to be modeled after FOIA Exemption 4's jurisprudence as set out in the Critical Mass decision, supra,[643] perhaps in deference to the fact that not all of the federal circuits have adopted the D.C. Circuit's well-reasoned opinion.

Criticism of the Critical Infrastructure Information Act

The CIIA has been criticized both for its inclusiveness as well as for its exclusiveness.

Stephen Gidiere and Jason Forrester wrote in 2002:

> The [CIIA] has been severely criticized as creating a major new loophole to FOIA's right of public access. But whether the [CIIA's] disclosure exemption is either "new" or "major" is subject to debate. In fact, much, if not all, of the information that falls within the ambit of the [CIIA]

642 *Id.*
643 975 F.2d 871 (D.C. Cir. 1992) (en banc).

> may be protected already by Exemption 4.[644]

Gidiere and Forrester appear to write from the standpoint that, while the new statute may be largely redundant given the legal framework, it is at least well intentioned. Other commentators, however, have been pointedly more critical:

> Present and future efforts to erode FOIA will harm requesters who are entitled to most of the information they seek. With the broad new CIIA FOIA exemption and a DOJ that will vigorously defend almost all agency FOIA decisions, the time period for responding to the requesting public could expand greatly, especially in light of preexisting backlogs and the amount of time it could take for administrative appeals and further litigation. The significance of September 11, 2001 and its impact on the freedom of information cannot be ignored--it has affected the perception of privacy, congressional lawmaking, and perhaps even court decisions. But this does not justify the expansion of governmental secrecy post-September 11, 2001. One would be hard-pressed to find a spokesperson for the notion that even sensitive information should flow unimpeded to the public in the name of governmental transparency. We all want to keep our country secure and our people safe, but the exemption framework codified at 5 U.S.C. § 552 protects adequately against the release of sensitive data that could place the U.S. at risk. [I]n this era of increased government secrecy…governmental transparency appears to have become a casualty of war. Only time will reveal the effects of these new restrictions on the public's right to government information. As long as the Bush Administration and Congress refuse to work within the adequate preexisting FOIA framework to address national security concerns, the prospects for governmental transparency in this new era appear grim.[645]

Indeed, the new legislation, while very broad in purpose, is still "voluntary" and, even though it purports to apply to critical infrastructure information in the hands of state and local governments, such an attempt to usurp the broad protections of the Tenth Amendment is likely to fail to pass Constitutional muster.[646]

The CIIA provides that critical infrastructure information "shall not, if provided to a State or local government…be made available pursuant to any State or local law requiring disclosure of information or records…otherwise be disclosed or distributed to any party by said State or local government…"[647] The Tenth Amendment states, "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved for the States respectively, or to the people."[648] The Tenth Amendment does not give Congress authority to require states to regulate, no matter how powerful the federal interest involved.[649] Rather, the Constitution gives Congress the authority to regulate matters which are directly within its purview, and to preempt contrary state regulation.[650]

The Supreme Court has recently reiterated these constitutional principles in the field of telecommunications facilities. In Nixon v. Missouri Mu-

644 Stephen Gidiere & Jason Forrester, *Balancing Homeland Security and Freedom of Information*, 16 Nat. Resources & Env't 139, 139 (Winter 2002).

645 Kristen Elizabeth Uhl, Comment, *The Freedom Of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, And Homeland Security*, Am. U. L. Rev., Oct. 2003 (citations omitted).

646 *See*, e.g., James T. O'Reilly, Federal Information Disclosure, Ch. 27, "State Information and Access Laws" (3d ed. 2007).

647 6 U.S.C. § 131, et seq. (Amended July 7, 2004).

648 U.S.C.A. Const. Amend. 10.

649 New York v. U.S., 505 U.S. 144 (1992).

650 *See id.*

nicipal League,[651] the Federal Communication Commission ("FCC") attempted to preempt a Missouri statute which prevented its municipalities and public utilities from providing telecommunications services or facilities. In holding for the state, the Court stated, "[F]ederal legislation threatening to trench on the States' arrangements for conducting their own governments should be treated with great skepticism, and read in a way that preserves a State's chosen disposition of its own power…"[652] The Court also pointed out that upholding the FCC provision "would treat States differently depending on the formal structures of their laws…"[653] Consequently, the CIIA appears to be infirm not only on constitutional grounds, but in its application with respect to the varying state open records laws. And when we recall that much of the nation's critical infrastructure is indeed owned by the state and local governments; a cursory review of their attempts to protect this information is in order.

State Open Records Laws

Many states moved, after September 11, 2001, to provide more protection to the flow of information related to critical infrastructure.[654] In Texas, the Government Code has been amended to protect broad categories of information, including documents which "identify the technical details of particular vulnerabilities of critical infrastructure."[655] Further, the Texas Attorney General has determined that "utility, drainage and engineering plans" of a Citigroup data processing center were protected from disclosure under state law, and that the data processing center was determined to be critical infrastructure.[656] Other states have gone even farther. Alabama, for example, has exempted from public disclosure:

> Records concerning security plans, procedures, assessments, measures, or systems, and any other records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures, including without limitation information concerning critical infrastructure (as defined in 42 U.S.C. § 5195c(e)…[657]

While this statute is exceptionally broad, not all of the states have followed suit. For example, no statutes relating to the additional protection of critical infrastructure were found on the books in Hawaii, Minnesota, Mississippi, Montana, New Hampshire, Rhode Island, and South Dakota. In New York, a 2004 law pertains to the reporting of security efforts by power generation and transmission facilities; however, the statute states that it is subject to New York's open records law, the Freedom of Information Law ("FOIL").[658] On the opposite coast in California, Governor Arnold Schwarzenegger signed legislation exempting "vulnerability assessments" from disclosure, as well as information related to facility security that "could be used to aid a potential terrorist or other criminal attack."[659]

Perhaps the inconsistent, and in some cases laissez-faire, attempts by the statehouses at protecting critical infrastructure is based on a reliance of the sweeping federal legislation. Or perhaps some states balance the public's right to access information above the perceived threat to public safety and security posed by disclosure. In New York, because the subway has been in existence since 1904,[660] and much of the City's other infrastruc-

651 541 U.S. 125 (2004).
652 Id. at 140.
653 Id. at 138.
654 A relatively comprehensive listing of these statutes can be found in a publication by the St. Mary's University School of Law Center for Terrorism Law entitled State Open Government Law and Practice in a Post-9/11 World, Lawyers & Judges Pub. Co., Inc. (2007); *see also*, Thomson/West, "50 State Surveys Utilities/Telecommunications Utilities" (November 2006).
655 Tex. Gov't Code Ann. § 418.181.
656 June 25, 2004, Texas Attorney General Opinion.
657 Ala. Code § 36-12-40; *see also* § 31-9A-14.
658 N.Y. Stat. Law § A9718 (2004).
659 Cal. Gov't Code § AB1209 (2004).
660 *See* New York Metropolitan Transit Authority

ture is even older than that, one could argue that there is little critical infrastructure information left to protect. Meanwhile, in Nevada, home of Las Vegas and the Hoover Dam, the Legislature has enacted some of the most sweeping critical infrastructure legislation which exempts "[d]rawings, maps, plans or records that reveal the critical infrastructure of primary buildings or facilities and other structures used for storing, transporting or transmitting water or electricity, natural gas or other forms of energy."[661]

The Problems with the Current State of the Law

The one inescapable conclusion of the above coast-to-coast study is that the states' collective efforts or non-efforts create a legal hodge-podge that is simply not rescued by the federal statute, given its questionable constitutional validity as it pertains to the states.[662] Indeed, the federal law has already been called into question in some instances. For example, the Maine Public Utilities Commission, in overruling AT&T's bid to withhold critical infrastructure information under the CIIA, stated that such federal legislation "does not limit the ability of a state agency to obtain such information independently."[663] Meanwhile, a New Jersey Administrative Law Judge ("ALJ") held that the CIIA exempted from disclosure a "digital copy format of the Brick Township Municipal Utilities Authority's GIS topographic mapping data."[664] In that case, however, the local governmental entity had voluntarily made the required submission and statement to the Department of Homeland Security ("DHS").[665]

The CIIA and the extant state open records laws together do not form an impenetrable shield for the protection of the nation's collective critical infrastructure information. Thus, a model solution should be implemented to address these weaknesses, and such that no one state is a weak link in the chain of critical infrastructure protection such that its assets could be seen as an easier target for a terrorist attack.

A Proposal for a Uniform Critical Infrastructure Information Protection Act

As a starting point, a Uniform Act could be modeled after the CIIA, and the following is an example of how such a model would begin:

> Critical infrastructure information that is voluntarily submitted to the state or any of its political subdivisions for use by the state or any of its political subdivisions regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—(A) shall be exempt from disclosure under this state's open records laws…

Additionally, a Uniform Act may want to increase the protection for critical infrastructure information by (1) adding specific protection for local public works projects; (2) providing that requesters provide identifying information; and (3) prohibiting the dissemination of critical infrastructure information via e-mail or other electronic means.

As suggested by Christopher Alonzi in the Spring 2005 Construction Lawyer, the standards found in the DHS and Department of Transportation ("DOT") regulations[666] "may establish a general standard of professional care or best practice that

("MTA") website at http://www.mta.info/mta/centennial.htm.

661 Nev. Rev. Stat. § 239C.210 (2003).

662 *See* supra text and notes at and after Note 41.

663 Me. Pub. Util. Comm'n. Order, Re Utility Service Area and Infrastructure Maps (Ch. 140), Docket No. 2001-284, 9 (May 7, 2003).

664 Robert Tombs v. Brick Township M.U.A., OAL DKT. NO. GRC 06786-04S (December 13, 2005).

665 *See id*. at 7.

666 *See* 49 C.F.R. pt. 15 (DHS) and 49 C.F.R. pt. 1520 (DOT).

should be followed…"[667] These standards seek to protect information related to critical infrastructure by, among other things, restricting its dissemination to "persons with a need to know."[668] They also require that such records be conspicuously marked and contain a disclosure limitation statement.[669] Finally, the C.F.R. provides for penalties for a failure to safeguard the protected information.[670] It is the suggestion here that such standards be incorporated into a Uniform Act regarding the protection of critical infrastructure as it pertains to local public works projects.

Further, requesters under the FOIA, or the Uniform Act proposed herein, could be required to file a form similar to the DoJ Form 361, "Certificate of Identity," such as is required with all Privacy Act requests.[671] This simple form asks that a person identify themselves sufficiently in exchange for the government's release of information. As referenced above, certain critical infrastructure information may be releasable to persons with a "need to know;" e.g., engineering firms, government contractors, etc.

In addition, neither the above referenced construction plans and specifications, nor any protected critical infrastructure information, should be sent electronically due to the dangers of interception and proliferation in cyberspace. The Oxford University website contains this common sense warning:

> Although we now take the email for granted, it is important to realise [sic] that - in its most basic form, at least - it is not necessarily a very secure or private means of communication. In fact, email has often been likened to the use of the postcard in conventional postal systems: it is open to being read or tampered with during transmission, and it might not even actually come from the person who apparently sent it.[672]

It is almost tautological that there is much danger in sending sensitive documents via e-mail in today's climate of sophisticated hackers and spammers.

Thus, even if one could draft a Uniform Act as set out above, the question becomes how to induce the states to incorporate it into their statutes. Given that the federal government has clearly taken the lead in this area, one approach would be the time-honored "carrot-stick" approach occasionally used by the federal government to promote uniform laws among the states in areas where it may not constitutionally mandate that they do so.

The federal government could offer a financial inducement to the states in terms of highway construction funding, as it did with the introduction of uniform speed limits on Interstate Highways, and in the implementation of a national drinking age of 21. The National Minimum Drinking Age Act of 1984[673] was passed on July 17, 1984 by Congress, and essentially required the states to legislate and enforce 21 years as the minimum age for purchasing or possessing alcoholic beverages. Under that federal statute, a state not enforcing the minimum age would be subjected to a ten percent decrease in its annual federal highway apportionment.[674]

This provision was challenged by South Dakota and found to be constitutional by the U.S. Supreme Court in the case of South Dakota v. Dole.[675] As the U.S. Supreme Court subsequently

667 Christopher H. Alonzi, *Protecting Security-Sensitive Plans and Specifications for Local Public Works Projects*, Constr. Law. (Spring 2005).
668 49 C.F.R. pt. 15.
669 *Id.*
670 *Id.*
671 Privacy Act of 1974, 5 U.S.C. § 552a.
672 Peter Higginbotham, Oxford University Computing Services, *Introduction to Security Issues in Email - PGP, S/MIME and SSL*, © Univ. of Oxford (February 2004), available at http://www.oucs.ox.ac.uk/email/secure.
673 23 U.S.C. §158.
674 23 U.S.C. §158(a)(1).
675 South Dakota v. Dole, 483 U.S. 203, 206-208

noted, "[T]here are a variety of methods, short of outright coercion, by which Congress may urge a State to adopt a legislative program consistent with federal interests. As relevant here, Congress may, under its spending power, attach conditions on the receipt of federal funds..."[676] Since this method of attempting to achieve legal uniformity throughout the states has passed constitutional scrutiny, it could be used to implement a Uniform Act in state open records laws.

Conclusion

Protecting critical infrastructure information in and of itself will not prevent terrorists from planning and attempting attacks on U.S. soil. However, the measure is a necessary link in the chain of national security and local public safety. By putting up legal roadblocks which our citizens with a legitimate need to know may circumnavigate, we may be saving countless lives by delaying a terrorist attack even for a few days or weeks. Those days and weeks may be all the precious time that intelligence and law enforcement authorities need to thwart a terrorist's plans to poison the water well or destroy some other asset of critical infrastructure. However, our current laws protecting critical infrastructure information should be made more consistent and exhaustive in their extent and in their applicability. In the current war on terror, that is not too high a price to pay.

5.3 Federal Preemption of State Open Records Laws After September 11

by Stephen Gidiere[677]

In the wake of the events of September 11, 2001, and the resulting international war on terrorism, governments in the United States at all levels—federal, state, and local—have changed the way they do business. Some of these changes are subtle; others dramatic. At the federal level, the Department of Homeland Security was created—the first new secretary-level executive department since the Department of Defense was created in 1947—causing a wholesale realignment of many federal agencies and their duties.[678] Some states have followed suit with similar structural changes.

In addition to changes in their own political structures, governments have modified the way they interact with each other. In the area of government records, one significant change in this regard is the increase in information sharing between and among federal, state, and local government officials. The need for sharing information as a method for preventing terrorism was memorialized, among other places, in the 9/11 Commission Report and a subsequent Executive Order on the subject.[679]

Despite the call for—and initiation of—increased sharing of homeland security related information since September 11, little attention has been paid to the legal problem of how to manage public access to such shared information as it changes hands. For example, when sensitive information is given to a state agency by a federal agency, do federal information laws follow that information? Or do state laws take over? Do both apply? The answers to these questions are some-

(1987).

676 New York v. U. S., 505 U.S. 144 (1992) (citing and discussing Dole).

677 Stephen Gidiere is a partner in the law firm of Balch & Bingham LLP, a southeastern regional law firm. Mr. Gidiere's practice encompasses a wide range of administrative law matters, including government information, environmental, and energy law. He is author of *The Federal Information Manual*, a book published by the American Bar Association about the Federal of Information Act and other federal information laws. He frequently publishes articles in the legal and popular press on a variety of information law topics.

678 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified at 6 U.S.C. §§ 101-557).

679 Final Report of the National Commission on Terrorist Attacks Upon the United States, § 13.1 (July 22, 2004); Exec. Order 13356, 69 Fed. Reg. 53599 (Aug. 27, 2004) (instructing the Director of Central Intelligence to develop common standards for sharing terrorism information with other agencies in the intelligence community, other agencies with counterterrorism functions, and state and local governments).

times not clear and often depend on the type of information at issue and who is providing it.

The general rule is that federal law preempts state law 1) if Congress passes a statute that expressly preempts state law; 2) if Congress preempts state law by occupation of the entire field of regulation; or 3) if the state law conflicts with federal law due to impossibility of compliance with state and federal law or when state law acts as an obstacle to the accomplishment of the federal purpose.[680] The first two instances are considered express preemption; the third is termed implied preemption. Thus, federal preemption could theoretically dictate what information held by states must be disclosed or protected from disclosure.

However, federal preemption has never had much of a place in the realm of open records laws.[681] As discussed below, for a variety of reasons, federal information laws generally do not preempt state open records laws. With limited exceptions,[682] this trend has continued even after September 11.

The purpose of this article is not to make a value judgment as to whether there should be more or less preemption of state open records laws, or to argue in favor of greater openness or secrecy in government. Rather, this article shows how certain aspects of current law and practice generally prevent federal preemption of state information laws and explores two approaches to federal-state relations that have developed in response to homeland security concerns.

I. The Federal-State Disconnect on Open Records

There is now, and always has been, a pronounced disconnect between federal and state laws regarding open records. Federal and state open records laws, in general, have nothing to do with each other, even though they may apply at times to the same document or information.

Consider, for example, the federal Freedom of Information Act (FOIA),[683] the overarching statute governing disclosure of federal records. FOIA requires the disclosure of any federal agency record to any person making a request for it, subject to nine statutory exemptions.[684] Several inherent features of FOIA limit its ability to control the flow of information that is exchanged or shared among federal and state governments.

First, FOIA is limited in application to federal agency records.[685] Under Supreme Court precedent, whether a particular document is an "agency record" depends on, among other factors, what entity or person controls the document. Under the two-part test established by the Supreme Court, a record is an "agency record" under FOIA if it is 1) created or obtained by an agency, and 2) in the agency's control.[686] As to the "agency control" requirement, the Supreme Court explained that "[b]y control we mean that the materials have come into

680 *See Freightliner Corp. v. Myrick*, 115 S.Ct. 1483, 1487 (1995); *Progressive Animal Welfare Society v. Univ. of Washington*, 884 P.2d 592 (Wash. 1995).

681 *See, e.g., Abbott v. Texas Dept. of Mental Health and Mental Retardation*, 212 S.W.2d 648 (Tex. App. 2006) (holding that federal Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations did not preempt state open records law); *Newsday, Inc. v. State Dept. of Trans.*, 10 A.D.3d 201 (N.Y.A.D. 2004) (holding that 23 U.S.C. § 409 did not preempt state open records law with respect to reports about hazardous intersections); *Progressive Animal Welfare Society v. Univ. of Washington*, 884 P.2d 592 (Wash. 1995) (holding that federal Freedom of Information Act does not preempt state law so as to require nondisclosure of unfunded grant proposal).

682 *See, e.g., ACLU v. County of Hudson*, 799 A.2d 649 (N.J. Super. 2002) (holding that regulation promulgated by United States Immigration and Naturalization Service preempted state law requiring disclosure of information about inmates in state prisons).

683 5 U.S.C. § 552.

684 *Id.*

685 *Id.* § 552(f)(2) (definition of "record").

686 *Tax Analysts*, 492 U.S. 136, 144-46 (1989). *See also Burka v. Department of Health and Human Services*, 87 F.3d 508, 515 (D.C. Cir. 1996).

the agency's possession in the legitimate conduct of its official business."[687] The Court of Appeals for the D.C. Circuit has established a more specific test to determine whether a given record is "in the agency's control." The D.C. Circuit considers four factors:

> 1) the intent of the document's creator to retain or relinquish control over the records; 2) the ability of the agency to use and dispose of the record as it sees fit; 3) the extent to which agency personnel have read or relied upon the document; and 4) the degree to which the document was integrated into the agency's record system or files.[688]

Accordingly, documents created by state or local governments and actually submitted to the federal government in the course of its official business may become agency records subject to disclosure under the FOIA once in the hands of the agency.[689] Moreover, a record may be in the constructive control of an agency and qualify as an "agency record."[690] Conversely, just because a document is in an agency's possession does not mean it is an agency record—for example, the creator of the document may not have intended to relinquish control over the document, and the document may thus only be "on loan" to the agency.

Second, even if FOIA's requirements did "follow" a particular record, FOIA only applies to *federal* agencies. The FOIA incorporates and refines the definition of "agency" contained in the Administrative Procedure Act (APA) (of which the FOIA is a part).[691] The APA generally defines "agency" to mean "each authority *of the Government of the United States*, whether or not it is within or subject to review by another agency, but does not include,[] for the purposes of the FOIA, Congress, United States courts, governments of United States territories or possessions, or the government of the District of Columbia…."[692] FOIA adds more description to this general definition. Under the FOIA, the term "agency as defined in [the APA] includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency."[693] Thus, states and local governments are not subject to FOIA, and their records are not either. The better reasoned decisions have held that FOIA does not preempt state open records laws.[694]

Even if states and their records were subject to FOIA, it would not necessarily result in the uniform treatment of homeland security related information. FOIA is a disclosure statute, not an information protection statute. In other words, FOIA itself does not require withholding of exempt material by entities subject to its disclosure requirement (other federal statutes may do so in some limited situations, a topic discussed later). Instead, agencies generally have discretion whether or not to invoke a FOIA exemption to avoid disclosure in a particular case.[695] This means that,

687 *Tax Analysts*, 492 U.S. at 145.

688 *Burka*, 87 F.3d at 515. (quoting *Tax Analysts v. Department of Justice*, 845 F.2d 1060, 1069 (D.C. Cir. 1988), *aff'd on other grounds*, 492 U.S. 136 (1989). *See also State of Missouri v. Department of the Interior*, 297 F.3d 745, 751 (8th Cir. 2002) (applying four factors from *Burka*).

689 *State of Missouri*, 297 F.3d at 750.

690 *Burka*, 87 F.3d at 515.

691 5 U.S.C. § 552(f).

692 *Id*. § 551(1)(A)-(D) (emphasis added).

693 *Id*. § 552(f)(1).

694 *Progressive Animal Welfare Society v. Univ. of Washington*, 884 P.2d 592 (Wash. 1995) (holding that federal Freedom of Information Act does not preempt state law so as to require nondisclosure of unfunded grant proposal). *But see Brady-Lunny v. Massey*, 185 F. Supp. 2d 928 (C.D. Ill. 2002) (holding that names of federal inmates need not be disclosed under state open records law because Exemption 7(C) of the FOIA protected such information).

695 *Chrysler Corp. v. Brown*, 441 U.S. 281, 293 (1979) ("We simply hold here that Congress did not design the FOIA exemptions to be mandatory bars to disclosure."). *See also Bartholdi Cable Co. Inc. v. Federal Communications Commission*, 114 F.3d 274, 282 (D.C. Cir. 1997) ("The fact that information falls within one of the FOIA

even if states were subject to FOIA, there could (and likely would be) uneven application of its exemptions given that they often require considerable interpretation to cover homeland security information.[696]

FOIA, of course, is not the only federal law dealing with the disclosure and protection of information. There is a host of other statutes making certain types of information either expressly public or confidential.[697] Courts have generally required that these statutes speak directly and expressly about prohibiting public disclosure in order for federal preemption to apply.[698]

II. Two Case Studies in Federal Preemption: CEII and CII

Two different case studies illustrate how the issue of federal preemption has been handled (or not handled) in the context of homeland security related information since September 11. The first involves a regulatory initiative by the Federal Energy Regulatory Commission ("FERC") to protect "critical energy infrastructure information" or "CEII." The second involves a statutory program administered by the Department of Homeland Security ("DHS") that protects "critical infrastructure information" or "CII." Although CEII and CII may actually cover some of the same kinds of information, they represent two very different approaches to the issue of federal preemption.

A. FERC and Critical Energy Infrastructure Information

Following September 11, FERC was one of the first federal agencies to formally revise its information handling and dissemination practices to reflect the threat of terrorism. FERC is an independent agency that regulates the interstate transmission of natural gas, oil, and electricity as well as the construction and operation of hydropower projects. FERC's primary statutory authorities for its regulatory activities are the Natural Gas Act ("NGA") and the Federal Power Act ("FPA"). In carrying out its mission, FERC collects information from regulated entities about the construction, design, operation, and vulnerabilities of facilities that generate and transport energy. FERC collects information in routine filings, like the Form 715 that operators of electricity transmission facilities must file annually, and also as part of its enforcement and compliance activities.

After September 11, FERC immediately recognized that much of the information it collects and makes available could be useful to a terrorist plotting an attack against American infrastructure. Within a month of the September 11 attacks, FERC issued a statement of policy announcing that it would remove from its website and public reading room "documents, such as oversized maps, that detail the specifications of energy facilities licensed or certified under [Part I of the Federal Power Act and Section 7(c) of the Natural Gas Act]."[699] FERC's action "affected tens of thousands of documents."[700]

exemptions does not necessarily mean that the agency cannot disclose the material. FOIA's exemptions simply permit, but do not require, an agency to withhold exempted information from the public.").

696 Stephen Gidiere & Jason Forrester, *Balancing Homeland Security and Freedom of Information*, 16 Nat. Resources & Env't 139 (2002). (analyzing potential application of FOIA Exemptions 1, 2, 4, and 7 to homeland security related information).

697 *See, e.g.*, P. Stephen Gidiere III, *The Federal Information Manual*, Appendix 8-1 (Amer. Bar Assoc. 2006) (cataloging dozens of statutes other than FOIA that deal with information protection).

698 *Compare ACLU v. County of Hudson*, 799 A.2d 649 (N.J. Super. 2002) (holding that regulation promulgated by United States Immigration and Naturalization Service preempted state law requiring disclosure of information about inmates in state prisons), *with Abbott v. Texas Dept. of Mental Health and Mental Retardation*, 212 S.W.2d 648 (Tex. App. 2006) (holding that federal Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations did not preempt state open records law).

699 66 Fed. Reg. 52917 (Oct. 18, 2001).

700 68 Fed. Reg. 9857, 9858 (March 3, 2003).

FERC followed up this initial move with a rulemaking to formalize changes to its information policy. On January 16, 2002, FERC issued a Notice of Inquiry (NOI) that set out its general position on the treatment of previously-public documents and sought public input on a series of related questions.[701] The NOI was intended to "assist the Commission in determining what changes, if any, should be made to its regulations to restrict unfettered general public access to critical energy infrastructure information, but still permit those with a need for the information to obtain it in an efficient manner."[702] Ultimately, FERC amended its regulations to create a new category of protected information known as "critical energy infrastructure information" or "CEII."[703]

The intricacies of the CEII rulemaking and its implementation are beyond the scope of this article. Two aspects of the rule, however, are important to note before considering how the rule deals with the issue of federal preemption. First, the rule only applies to certain types of information about critical energy infrastructure *that is otherwise exempt from disclosure under the FOIA*.[704] Therefore, for CEII, the issue of how to deal with information that may be shared with a variety of government entities reflects the limitations inherent in the FOIA, as discussed in Section I. Second, the rule does not prohibit all public access to CEII, but instead sets certain conditions on release such as the execution of a non-disclosure agreement.[705]

FERC struggled with the issue of federal preemption from the beginning of the CEII rulemaking. The issue was particularly relevant for FERC because state agencies, such as state public service commissions, also have regulatory jurisdiction over owners and operators of energy facilities and thus collect and maintain CEII. Complicating the matter even further, both the FPA and the NGA contain provisions obligating FERC to make certain information available to the state commissions.[706]

Thus, FERC had to decide the level of access to CEII that state commissions would receive and whether the restrictions on use that apply to other requesters, such as those contained in non-disclosure agreements, would apply to state commissions. The issue of federal preemption is at the heart of this dilemma. In the CEII NOPR, FERC cautiously asserted that "the Federal FOIA law may trump state FOIA law where the information at issue is Federal information."[707]

The single case cited by FERC for this proposition, however, did not stand for such a sweeping statement.[708] In response to commenter's concerns, FERC clarified in the final rule that preemption would only apply "to state agency requests to FERC for CEII that the Commission had generated or collected."[709] But FERC further explained that "[i]t does not make sense for the Commission to release information to the State

701 67 Fed. Reg. 3129 (Jan. 23, 2002).
702 *Id.*
703 67 Fed. Reg. 57994 (Sept. 13, 2002) (notice of proposed rulemaking); 68 Fed. Reg. 9857 (Mar. 3, 2003) (final rule) (codified at 18 C.F.R. §§ 388.112, .113). 28 18 C.F.R. § 388.113(c)(1).
704 18 C.F.R. § 388.113(c)(1).
705 18 C.F.R. § 388.113.
706 *See, e.g.*, 16 U.S.C. § 824h(c) (Federal Power Act); 15 U.S.C. § 717p(c) (Natural Gas Act).
707 67 Fed. Reg. at 58002.
708 The case FERC cited—*United States v. Napper*, 887 F.2d1528 (11th Cir. 1989)—holds that a state agency may be required to return a record to the federal agency it was received from upon receipt of a request for the record under state law. More recently, Congress addressed the concept of federal agencies "loaning" records to state agencies in one specific context when it created by statute a class of protected information termed "sensitive homeland security information" or "SHSI" as part of the Homeland Security Information Sharing Act (HSISA), Pub L. No. 107-296, §§ 891-899, 116 Stat. 2252 (codified at 6 U.S.C. §§ 481-484). Congress provided that "information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information." 6 U.S.C. § 482(e).
709 68 Fed. Reg. at 9865.

Agencies with no agreement to protect the information, at least to the extent permitted by law."[710] Thus, FERC required state commission to follow the same request procedures for CEII as any other requestor. This includes submitting a written request to the CEII Coordinator and demonstrating a need for and willingness and ability to protect the information. FERC will presume that state commissions "have a need to know information within their state involving issues within their responsibilities."[711] A nondisclosure agreement with a state agency will contain provisions requiring the agency to give FERC notice of any request for the CEII under state law,[712] thus giving FERC the opportunity to "take action to prevent release of the information."[713]

So, in the end, FERC did not rely on federal preemption at all. Instead, it adopted a practical approach of controlling possession and application of state disclosure laws through the use of nondisclosure agreements and advance notice of a request under state law.

B. DHS and Critical Infrastructure Information

Congress took a very different tack when it created statutory protection for a class of information termed "critical infrastructure information" or "CII." CII is a class of information created by a subtitle of the Homeland Security Act of 2002 designated the Critical Infrastructure Information Act of 2002 (CIIA).[714] The statute defines CII as "information not customarily in the public domain and related to the security of critical infrastructure[715] or protected systems."[716] CII that is voluntarily provided to a "covered federal agency" (DHS is the only such agency at present) is protected from, among other things, disclosure by any federal agency under the FOIA.[717] So, in FOIA parlance, the HSA contains a new FOIA Exemption 3 provision protecting CII.[718] The CII program is administered by DHS, and DHS has issued final rules that detail how CII is to be submitted, marked, handled, and shared.[719]

A purpose of the CII designation is to foster sharing of information about critical infrastructure, much of which is possessed by the private sector. By providing protection from public disclosure, the statute seeks to encourage the private sector to voluntarily share information that it otherwise would not. In order to achieve the ultimate goal of preventing or responding to terrorism, CII collected by DHS must be shared with other federal officials, state and local governments, and members of the private sector, as appropriate. It's at this point that the thorny and persistent problem of how to extend federal protection for the information comes into play.

For CII, Congress tackled the problem head on. CII, Congress provided, "shall not, if provided to a State or local government or government agency [] be made available pursuant to any State or local law requiring disclosure of information or records [or] otherwise be disclosed or distributed to any party by said State or local government agency without the written consent of the person or entity submitting such information."[720]

710 *Id.*
711 *Id.*
712 *Id.* at 9866.
713 *Id.*; 67 Fed. Reg. at 58002 (citing *United States v. Napper*, 887 F.2d at 1530 (11th Cir. 1989)).
714 Pub. L. No. 107-296, §§ 211-215, 116 Stat. 2150 (codified at 6 U.S.C. §§ 131-134).
715 The HSA defines "critical infrastructure" by cross-referencing the definition of that term in the USA PATRIOT Act, Pub. L. No. 107-56, § 1016(e), 115 Stat. 401 (codified at 42 U.S.C. § 5195c(e)). *See* 6 U.S.C. § 101(6).
716 6 U.S.C. § 131(3).
717 *Id.* § 133(a)(1).
718 *See* Section 8.3 (discussing FOIA Exemption 3).
719 71 Fed. Reg. 52262 (Sept. 1, 2006) (codified at 6 C.F.R. Part 29).
720 6 U.S.C. § 133(a)(1)(E)(i), (ii).

In its final rule, DHS imposed even more specific requirements on States and local governments receiving CII. DHS's rules say that "State and local governments receiving [CII] will acknowledge in such arrangements the primacy of [CII] protections under the CII Act; agree to assert all available legal defenses to disclosure of [CII] under State, or local public disclosure laws, statutes or ordinances; and will agree to treat breaches of the agreements by their employees or contractors as matters subject to the criminal code or to the applicable employee code of conduct for the jurisdiction."[721]

Thus, the CII provision seems to be a clear statement of Congress' intent to completely preempt state open records laws with respect to CII. At a minimum, this provision and the implementing DHS regulations result in implied federal preemption because it would be impossible to comply with both this federal law and a state open record law calling for disclosure.

III. Conclusion

Few would dispute that strong federal leadership is needed to combat and respond to terrorism. Unlike with economic or social policy, defense against terrorism is not one of those areas of government that lends itself to the proverbial "states as laboratories" approach. And with information disclosure, in particular, public release of a piece of information by just one jurisdiction would render moot efforts by other jurisdictions to keep the information confidential—once information is in the public domain, it is difficult if not impossible to bring it back. And, in fact, while states could voluntarily recognize federal laws and prohibitions regarding homeland security information in their own open records statutes ensuring uniformity, few states have actually done so.[722] If we want a uniform approach to the handling and disclosure of sensitive homeland security information, federal preemption is a practical necessity.

Many would dispute, however, that federal law should step in to comprehensively (or even selectively) preempt state law in the area of open records. And, by and large, this has not happened since September 11. The case of CII thus stands as an outlier in information law—a clear preemption of state disclosure laws for a specific type of homeland security information. The CII provision has come under sharp criticism, as an overly broad and unnecessary new disclosure exemption.[723] But few could argue that Congress' and DHS's clear commands about CII are not a more efficient approach to information control as compared, for example, to relying on a fiction that federal information is simply "on loan" to a state or local government and can be retrieved to avoid a public request under state law.

Even with six years of perspective and experience since September 11, it is hard to say which approach—or combination of approaches—works best to encourage information sharing among all levels of government while protecting from public disclosure only that information that truly deserves protection. Thorny questions of federalism and separation of powers have existed in this country since—and before—its inception. Nothing has happened in the years since September 11 to suggest that those questions will subside. In fact, the back and forth of the federalism debate is

721 6 C.F.R. § 29.8(b).

722 For a review of how states have responded to September 11 in amending or not amending their open records laws, *see generally* The Reporters Committee for Freedom of the Press, State Open Government Law and Practice in a Post-9/11 World (2007). Most states that have amended their open records laws to protect more information post9/11 have done so by enacting their own unique exemptions. At least one state, however—Alabama—has opted to follow the federal lead on protecting information about critical infrastructure and has incorporated directly into state law the federal law on "critical infrastructure" and "critical energy infrastructure information." *See* Ala. Code § 36-12-40.

723 *See, e.g.*, Kristen Elizabeth Uhl, *The Freedom of Information Act Post 9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security*, 53 Amer. Univ. L. Rev. 261 (2003).

in some ways the grease that keeps our democracy humming along. That debate is sure to continue.

5.4 Federal Freedom of Information Act-Driven Coverage of the Department of Homeland Security: A Pilot Study

by Charles N. Davis, Ph.D.

Without question, one of the most important developments in the new century has been the United States' response to the horrific terrorist attacks of Sept. 11, 2001. While much scholarly attention has been devoted to coverage of the global conflagrations attendant to the war on terror, relatively little attention has been paid to coverage of the creation of one of the world's largest bureaucratic apparatuses – the Department of Homeland Security.

Congress and the President created the Department of Homeland Security ("DHS") in response to the September 11, 2001 terrorist attacks.[724] In the days following the terrorist attacks, a dizzying array of government employees from agencies throughout Washington and beyond scrambled to provide assistance to the Bush Administration.[725] The inevitable red tape and interagency communication barriers quickly gave rise to the idea that there should be one unified department to combat and respond to future terrorist attacks on U.S. soil.[726] In just over a year, that idea grew into a sprawling new Cabinet-level agency with a sweeping mandate, two dozen subordinate agencies and thousands of employees overseeing a vast multitude of programs.[727]

The creation of DHS marked the first major government restructuring since the creation of the Department of Energy in 1977, and the creation of the nation's third largest federal agency.[728] With an initial budget of $37 billion, DHS encompasses 170,000 workers from twenty-two agencies, including the Secret Service, Border Patrol, Coast Guard, and Customs Service.[729] The Department's mission to coordinate counter-terrorism measures and preemptive defense is carried out through the Department's four divisions: border and transportation security; emergency preparedness and response; countermeasures for chemical, biological, radiological, and nuclear attacks; and an intelligence clearinghouse.[730]

The massive dimensions of DHS, and its multi-agency structure, make it a daunting task for journalists to cover effectively. Its creation came with a blanket Freedom of Information Act ("FOIA") exemption for private industries sup-

724 Jessica Reaves, *Homeland Security: A Primer*, Time (Online Ed.), Nov. 19, 2002, *available at* http://www.time.com/time/nation/article/0,8599,391161,00.html [hereinafter Reaves].

725 *Id.*

726 *Id.* President Bush's initial proposal of a Cabinet-level Department of Homeland Security called for "substantially transforming the current confusing patchwork of government activities into a single department whose primary mission is to protect our homeland."

727 President Bush initially established an Office of Homeland Security by Executive Order on October 8, 2001. *See* Press Release, The White House, Executive Order Establishing Office of Homeland Security (Oct. 8, 2001). Senators Joseph Lieberman and Arlen Specter subsequently introduced Senate legislation to create a Cabinet-level Department of Homeland Security. *See* Press Release, Senate Committee on Governmental Affairs, Lieberman, Specter Offer Homeland Defense Legislation (Oct. 11, 2001), *available at* http://www.senate.gov/<diff>gov<uscore>affairs/101101homedefpress.htm. After President Bush officially supported the creation of a Department of Homeland Security in early June 2002, it was only a matter of time before the Homeland Security Act of 2002 ("HSA") passed in the House and Senate. The Homeland Security Act of 2002 passed the United States House of Representatives in July 2002, but disputes over workers' rights, as well as other controversial provisions, impeded passage until after the November 2002 elections gave both houses of Congress a Republican majority. *See* Kristen Elizabeth Uhl, *The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, & Homeland Security,* 53 Am. U.L. Rev. 261 (Oct. 2003).

728 General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security* 3, 2003, *available at* http://www.gao.gov/pas/2003/d03102.pdf.

729 *Supra* note 5, at 6.

730 Reaves, *supra* note 1.

porting the nation's critical infrastructure, yielding a great deal of critical editorial coverage early in the Department's history.

The critical infrastructure exemption in no way exempts the vast majority of DHS records, however, raising the question of how and to what ends journalists and other FOIA users are employing the Act to access documents from DHS and its agencies. To examine the use of FOIA within DHS, the researcher examined coverage of the Department and each of its major subsidiary agencies since its creation, looking specifically for coverage generated by use of FOIA. The purpose of this study is to determine how journalists have used FOIA to bring important information regarding the Department to the public's attention and to examine the nature and extent of information flow from DHS to the press and public. Knowing how journalists are using FOIA to access information about the Department is crucial to understanding the depth and breadth of information flow, and serves as an important barometer of how effectively the press is monitoring one of the most important functions of modern government. The use, or lack of use, of FOIA by journalists is a telling sign of the quality of coverage of homeland security by the American press.

Coverage of the Department and its agencies must be viewed in light of the fact that journalists have paid a great deal of attention to chronicling the increasing trend towards federal government secrecy over the last six years. Literally hundreds, if not thousands, of stories documenting the rise in federal governmental secrecy dominate any scholarly examination of the mass media treatment of the broader subject of FOIA. Without repeating all of the significant findings, the totality of the secrecy bears mention.

In the year following the September 11 attacks, the government classified 11.3 million documents, which jumped to 14.2 million the following year and 15.6 million the year thereafter.[731] The increase in pages classified was followed by stories detailing a substantial drop, since fiscal year 2001, in the number of previously classified pages that the government declassified.[732] Much journalistic attention was also devoted to the post-Sept. 11 trend of agencies removing government documents from web sites and publicly available databases.[733] The press also thoroughly reported the fact that federal agencies relied increasingly on statutory exemptions to deny requests for records sought under the FOIA.[734] According to a study of 22 agencies by the Coalition of Journalists for Open Government, the use of FOIA exemptions to deny requests jumped by 22 percent between the years 2000 and 2004, even though the total number of FOIA requests to these agencies dropped by 13 percent during the period studied.[735] Most surprisingly, the increase had no apparent connection to national security. Use of FOIA Exemption l, which protects classified information, actually dropped during this same period.[736]

Against such a backdrop of press opposition to federal secrecy, one would expect vigilance where the Department and its agencies are concerned. Indeed, had this study focused on editorial commen-

731 Peter M. Shane, *Symposium, Federal Secrecy Policy after Sept. 11 & the Future of the Information Society, Introductory Essay: Social Theory Meets Social Policy: Culture, Identity And Public Information Policy After September 11,* 2 ISJLP I (Winter 2005-2006), citing David Nather, *Classified: A Rise in 'State Secrets'*, 63 CQ WEEKLY 1958, 1960 (2005) [hereinafter Shane].

732 *Supra* note 8, citing Nather, at 1965.

733 John Podesta, *Need to Know: Governing in Secret*, *in* A Little Knowledge: Privacy, Security, & Public Information After Sept. 11, 11, 13-14 (Peter M. Shane, John Podesta, and Richard C. Leone, eds., 2004); Laura Gordon-Murnane, *Shhh!!: Keeping Current on Government Secrecy*, Searcher: The Magazine for Database Professionals, Jan. 2006, at 35, 36.

734 Coalition of Journalists For Open Government (CJOG), *When Exemptions Become the Rule* (undated document), at 2-3, *available at* http://www.cjog.net/documents/Exemptions_Study.pdf (last visited Sept. 1, 2007).

735 *Ibid.*

736 Shane, *supra* note 8, at 2.

tary rather than news content, the findings would have told a very different story, one of almost uniform opposition to federal information policy and increased secrecy, and one of robust support for greater openness under the FOIA. Analysis of news coverage utilizing FOIA tells quite a different story, however. Examination of the news coverage of a broad sample of American newspapers provides broad evidence that the press is vastly underutilizing the FOIA where the Department and its agencies are concerned.

Methodology

To examine coverage of the Department and its subsidiary agencies, the researcher conducted a series of Lexis-Nexis searches to identify a wide range of stories involving DHS and its major subsidiary agencies. To examine overall coverage of each agency, the researcher conducted searches of the top 10 U.S. newspapers by circulation[737] from November 2001 to August 15, 2007 for each of 20 distinct agencies.[738] Each article retrieved by the search was then reviewed to determine whether the content was discussing an issue generated by a FOIA request; glancing mentions of the Act and articles discussing FOIA generally were eliminated, as well as editorials, letters to the editor and other non-related content.

In addition to the agency-specific searches, the researcher also looked more broadly at national newspaper coverage by conducting a search in the general news library of Lexis-Nexis for all articles containing the terms "freedom of information" and "homeland security" from Sept. 1, 2007 to Sept. 1, 2005.[739] Each article was analyzed to determine whether the story was the result of a FOIA request, or merely a peripheral mention of the Act. The goal was to identify stories in which a FOIA request generated some portion of the article's content, and to exclude articles discussing the relative merits of FOIA or arguments for and against greater access, editorials and other related content.

After all the text was analyzed, the following questions were asked:

1. What was the role of FOIA in the story? Could it be said that FOIA served as the catalyst for the story?
2. If FOIA was used to obtain the information that served as the genesis of the story, what information was sought, and what information was obtained?
3. What agency or agencies produced the documents, and was there any indication of denial or redaction?
4. What subject(s) were covered by the story, and what did the FOIA-driven information add to understanding of the story?

737 The 10 newspapers, as ranked by the Audit Bureau of Circulation, are USA Today; The Wall Street Journal, The New York Times, The Los Angeles Times, Washington Post, Chicago Tribune, New York Daily News, Philadelphia Inquirer, Denver Post and Houston Chronicle. All but the New York Daily News and Philadelphia Inquirer are archived in Lexis-Nexis; those newspapers are available in the Newsbank database, which was searched as well.

738 Each newspaper was searched for all articles mentioning "freedom of information" and the following agency names: the Department of Homeland Security; the Federal Emergency Management Agency; U.S. Customs; the Transportation Security Agency; Immigration and Naturalization Service; the Federal Law Enforcement Training Center; the Animal and Plant Health Inspection Service; the Office for Domestic Preparedness; the Strategic National Stockpile and/or National Disaster Medical System; the Nuclear Incident Response Team; the Domestic Emergency Support Teams; the National Domestic Preparedness Office; CBRN Countermeasures Programs; Environmental Measurements Laboratory; the National BW Defense Analysis Center; the Plum Island Animal Disease Center; the Federal Computer Incident Response Center; the National Communications System of the Department of Defense; the National Infrastructure Protection Center; the Energy Security and Assurance Program; the Secret Service; and the United States Coast Guard. The departments were obtained from a DHS web page entitled "History: Who Became Part of the Department?" available at http://www.dhs.gov/xabout/history/editorial_0133.shtm

739 The general news search was limited to a two-year timeframe by the Lexis-Nexis database, yielding 2,129 articles. Of those, 1,601 articles were eliminated, leaving 528 articles for the analysis.

As with all qualitative analyses, the results will be subjective. The success of this study can only be judged by how persuasive, informative and comprehensive the analysis is. The results offer a detailed snapshot – albeit an unscientific sample – of the use of FOIA to examine DHS and its subsidiary agencies by journalists.

Findings

Agency Coverage: 2002-2007

The dominant theme of the findings overall is a relative paucity of FOIA-driven coverage of DHS and its subsidiary agencies. While isolated areas of the massive agency have generated some FOIA-driven coverage, much of the coverage can best be described as episodic and fleeting in nature. Few, if any, American newspapers are devoting regular reporting resources to any of the 20-plus entities encompassing the homeland security apparatus, and the result is a lack of any sense of systematic journalistic scrutiny using FOIA to inform the public of the operations of one of the nation's most critical governmental operations.

The agency-specific content searches provide the most convincing evidence of a relative lack of FOIA-driven coverage. Overall, the researcher found just 60 FOIA-driven stories from the first mentions of DHS in 2001 to present (August 2007) – in 23 agency searches for the agency name and "freedom of information" – in each of the top 10 U.S. newspapers in circulation – a total of 230 searches.

Of the 230 searches, only nine agencies yielded any FOIA-driven coverage: the Animal and Plant Health Inspection Service; the United States Coast Guard; the United States Customs Service; the Department of Homeland Security (general search); the Federal Emergency Management Agency; the Immigration and Naturalization Service; the Office for Domestic Preparedness; the United States Secret Service; and the Transportation Security Administration.

The following agencies yielded no FOIA-driven coverage from 2001-2007: the Federal Law Enforcement Training Center; the Strategic National Stockpile and/or National Disaster Medical System; the Nuclear Incident Response Team; the Domestic Emergency Support Teams; CBRN Countermeasures Programs; Environmental Measurements Laboratory; the National BW Defense Analysis Center; the Plum Island Animal Disease Center; the Federal Computer Incident Response Center; the National Communications System of the Department of Defense; the National Infrastructure Protection Center; the Energy Security and Assurance Program; and the United States Coast Guard.

Given the range of agencies, the number of news stories examined and the length of time under examination, it is clear that few stories utilizing FOIA to again access to records target DHS or its subsidiary agencies. Of the nine agencies that produced the 60 FOIA-driven stories, none was the subject of more than a dozen stories, and the Animal and Plant Health Inspection Service and the Office for Domestic Preparedness were the subject of three stories and one story, respectively. The heaviest coverage, beyond that for DHS itself (18 stories), was directed at the Secret Service (13 stories); the TSA (5 stories); and FEMA (5 stories).

Though surprisingly small, the agency-specific coverage contained several examples of stories that shed light on important news regarding the Department and its activities. For example, The New York Times used FOIA to document the role of contractors across the government, including DHS, using records to demonstrate that competition, intended to produce savings, appears to have sharply eroded. The analysis by The New York Times shows that fewer than half of all ''contract actions'' -- new contracts and payments against

existing contracts -- are now subject to full and open competition. Just 48 percent were competitive in 2005, down from 79 percent in 2001, the story said.[740]

Another important contracting story used FOIA to reveal the contents of a federal audit that calls into question $303 million of the $741 million spent to assess and hire airport passenger screeners for the Transportation Security Administration after the terrorist attacks of Sept. 11, 2001.[741] The story details how officials at the fledgling agency lost control of the spending in the rush to hire 60,000 screeners to meet a one-year congressional deadline. The audit, performed by the Defense Contract Audit Agency at the TSA's behest, spotlights scores of expenses: $20-an-hour temporary workers billed to the government at $48 per hour, subcontractors who signed out $5,000 in cash at a time with no supporting documents, and $4.4 million in "no show" fees for job candidates who did not appear for tests.

Given the centrality of border security and the important role that the U.S. Customs Service and Immigration and Naturalization Service play in the roiling debate over immigration policy, surprisingly few stories using FOIA to cover either agency have appeared in the years since the creation of DHS. The stories that have appeared provided important glimpses into agency policy, and suggest that many similar stories merit attention from the press.

For example, a May 2007 Associated Press story relied on FOIA-driven analysis by the Transactional Records Access Clearinghouse showing that U.S. immigration officials tried to deport only 12 people on terrorism-related charges from 2004 through 2006. That group of 12 represented "a tiny fraction of the 814,073 people the government tried to remove from the country during those three years," the story said, while acknowledging the figure understates the anti-terrorism effort by the Homeland Security Department's immigration agencies.[742] The story offered a brief, though informative look at a rather significant data set obtained through the FOIA – data that could be used by reporters to tell a variety of stories about the enforcement efforts of two DHS agencies, Immigration and Customs Enforcement and Customs and Border Protection.

A 2003 Denver Post story used the FOIA to obtain documents central to an underreported issue stemming from DHS immigration enforcement efforts: bed space for illegal immigrants detained by authorities.[743] The story provided an excellent overview of the nationwide expansion of a DHS program critical to immigration enforcement that would help security officials hold as many as 8,000 more suspected illegal immigrants a day. The story found that the current population of about 22,000 detainees represents the fastest-growing segment of America's federal prison population, and used records to inform readers of an important, though certainly controversial, DHS policy.

Another intriguing 2003 story by the Associated Press tracked federal prosecutions of terrorism cases since the Sept. 11 attacks, using FOIA-generated documents to show that such prosecutions have increased tenfold since authorities expanded the types of crimes classified as related to terrorism or international security.[744] The AP again used

740 Scott Shane & Ron Nixon, *In Washington, Contractors Take On Biggest Role Ever*, N.Y. Times, Feb. 4, 2007, A1.

741 Scott Higham & Robert O'Harrow Jr., *The High Cost of a Rush to Security; TSA Lost Control of Over $300 Million Spent by Contractor to Hire Airport Screeners After 9/11*, N.Y. Times, June 30, 2005, A1.

742 Michael J. Sniffen, *Study questions deportation effort; Few people were targeted on charges related to terrorism*, Associated Press *in* Houston Chronicle, May 28, 2007, A8.

743 Bruce Finley, *More prison beds for migrants Feds seek space to accommodate crackdown on illegal immigration*, Denver Post, Dec. 7, 2003, A1.

744 David Pace, *Terror-connected crime stats soar; Prosecutions up tenfold since 9/11; INS, Social Security play big role*, Associated Press *in* Houston Chronicle, Feb. 14, 2003, A2.

TRAC data obtained by the FOIA, concluding that during the year that began 19 days after the attacks on New York and Washington, federal prosecutors charged 1,208 individuals with crimes they classified as related to terrorism or international security, compared with 115 the previous year.

The story found that the focus on terrorism prevention and prosecution hadn't appeared to have drained resources away from other federal law enforcement activities, as many experts, including then-U.S. Attorney General John Ashcroft, predicted shortly after Sept. 11, 2001. The TRAC data showed that terrorism-related prosecutions accounted for just 1.3 percent of all federal criminal cases in 2002. Prosecutions for all types of crimes increased by 3.6 percent in 2002, with terrorism cases accounting for one-third of that total. The story also noted that TRAC obtained the records after a two-year court battle with the Justice Department over the Freedom of Information Act.

Given TRAC's systemic use of the FOIA to aggregate enforcement data, it is surprising that numerous stories in subsequent years utilizing the data were not produced. The fleeting attention paid to such an important story is inexplicable, given the availability of the data and the importance of the topic, yet the researcher found less than 10 media mentions of the data from 2004 to August 2007.

Given its highly public profile and resonance in the American psyche following the Sept. 11 attacks, it's not surprising that the Transportation Security Administration's airport security apparatus has generated as much FOIA-driven coverage as any DHS agency. A number of stories used TSA records to break stories about enforcement issues at American airports, demonstrating the effectiveness of the FOIA in obtaining a wide range of information about one of the most visible and important parts of the DHS.

For example, a 2003 Washington Post story informed readers that Los Angeles International Airport officials uncovered 12 airport screeners with felonies or other criminal backgrounds just weeks after the federal government said it "rescrubbed" the backgrounds of its workforce there.[745] Several of the 12 screeners working for the TSA had criminal records related to "unlawful, use, sale, distribution or manufacture of an explosive or weapon" and held security badges that provide access to secure areas of the airport for more than 200 days in most cases.[746]

Documents obtained under a FOIA request showed that the 12 screeners, who "were certified by the TSA as not having a disqualifying history," were later determined by the airport to "have a disqualifying criminal history." An additional 59 out of more than 2,000 screeners were flagged for further review of their pasts after the airport conducted fingerprint-based checks.

Another impressive use of FOIA-generated documents examined air security fines at airports across the country, finding wide disparities in TSA's penalties for carrying banned items. The Wall Street Journal's 2005 story examined data on fines from across the nation, concluding that while those carrying banned items face the potential for heavy fines, the reality depended a great deal on the airport in question.[747]

The documents provided a great deal of telling anecdotes for the reporter, who used them to provide a highly informative look at the TSA's fines:

> At the airport in Manchester, N.H., last year, for instance, nearly 700 people were

745 Sara Kehaulani Goo, *Airport Finds That More Screeners Are Questionable*, Wash. Post, June 12, 2003, A3.

746 *Ibid.*

747 Laura Meckler, *Air-Security Fines Under Scrutiny --- Analysis of Data Finds Wide Disparities In TSA's Penalties for Travelers Carrying Banned Items*, Wall St. J., June 28, 2005, D1.

> fined for carrying prohibited items, while at Seattle-Tacoma International Airport -- which had nearly 12 million more people passing through security during that time -- just 35 penalties were issued. At New York's La Guardia, 286 passengers were fined last year. But just a few miles away, at John F. Kennedy International Airport, only 83 people were penalized.

Overall, the story showed that fines are rare -- the vast majority of people who try to bring prohibited items through airport security aren't fined at all. In 2004, the TSA collected more than seven million prohibited items from passengers, of which 81,600 were firearms, explosives, box cutters and knives with blades over three inches. But it levied fewer than 14,000 fines altogether in 2004, the story said.

General Coverage: 2005-2007

To gain a better sense of the national coverage in a broader spectrum of news media, the researcher conducted a search in the general news library of Lexis-Nexis for all articles containing the terms "freedom of information" and "homeland security" from Sept. 1, 2007 to Sept. 1, 2005.[748] Each article was analyzed to determine whether the story was the result of a FOIA request, or merely a peripheral mention of the Act. The goal was to identify stories in which a FOIA request generated some portion of the article's content, and to exclude articles discussing the relative merits of FOIA or arguments for and against greater access, editorials and other related content. The general news search was limited to a two-year timeframe by the Lexis-Nexis database, yielding 2,129 articles. Of those, 1,601 articles were eliminated, leaving 528 articles for the analysis.

The breadth of the more recent coverage across the 100-plus newspapers archived in the Lexis-Nexis database offered a more diverse cross-section of coverage on a far wider range of topics. Despite the fact that the search generated far more coverage overall, the episodic nature of most of the coverage made it difficult to detect much in the way of any systemic, repeated coverage of DHS. Many stories were isolated instances of FOIA use by a single newspaper or wire service, yet the far more aggressive use of the FOIA to produce news coverage of the agency is noteworthy for it reveals several productive information flows that demonstrate the effectiveness of the Act.

To be sure, there are excellent examples of the FOIA being utilized by journalists to tell important stories about the DHS. The Department's grants program was the subject of a number of informative stories, some fueled by records obtained by reporters using state public records laws and the federal law, while others documented the secrecy surrounding the grants in their state. For example, an August 1, 2004 Denver Post story detailed reporters' unsuccessful efforts to learn what Colorado's $122 million in anti-terrorism funding was used for, even in the broadest terms.[749]

Colorado officials denied the Post access to any information about what state first-responders bought with those funds, and noted that other states have made such records public. The story noted that the volunteer fire department in tiny Estes Park, Colo., won a grant for $88,000 in 2002, citing a records request granted by the federal Homeland Security Department.[750] The story noted that the funds were used for health screenings and personal training, prompting discussion of the merits of such spending where infrastructural shortages exist. Regardless of the relative merits of the program, which state and local officials defended as a much-needed defense against firefighter health

748 The general news search was limited to a two-year timeframe by the Lexis-Nexis database, yielding 2,129 articles. Of those, 1,601 articles were eliminated, leaving 528 articles for the analysis.

749 Chuck Plunkett, *Anti-terror funds under fire*, Denver Post, Aug. 1, 2004, C-01.

750 *Ibid.*

issues, the debate is a useful example of the utility of such records and evidence of the potential for the press and public to access such records from the federal agency.

The Chicago Daily Herald also used the FOIA to access hundreds of records detailing homeland security spending in 127 metropolitan Chicago communities, producing a detailed look at the many uses of grant funds, from protective gear for first responders to a $12.85 million communication system for Cook County, Illinois.[751] The analysis raised several important questions about spending priorities and approaches in funding homeland security at the local level, and included a community-by-community listing of purchases. A companion story documented the inability of many of the communities to respond adequately to the information requests, highlighting the fact that access to local homeland security spending records often is not a federal DHS issue, but one of compliance with state FOI laws.[752] The city of Chicago – which had received $65.8 million from 2002 to 2005 – refused to detail even general areas in which the money was spent.[753] Several other stories used funding records obtained from DHS and state homeland security agencies to explore spending in Michigan[754] and New Jersey,[755] for example.

Several stories illustrated the uneven nature of access to records under state public records laws. The Journal News of Westchester County, New York, provided a telling illustration in a 2005 story detailing the newspaper's difficulties in obtaining bridge inspection data – a story with added importance given the Minneapolis bridge collapse this summer.[756] Faced with denials of the data in New York, reporters sought the same data for the Golden Gate Bridge, and received a complete copy of the 35-page report from California state officials via e-mail. While the reporters received most of the report from the Port Authority of New York and New Jersey, officials redacted substantial portions of the document, citing homeland security concerns. The story provided a comparative approach to access laws seldom seen in the coverage, launching an important discussion about safety and secrecy.

A story in Pitch Weekly, the New Times weekly in Kansas City, offered a blow-by-blow account of a reporter's futile attempts to gain access to records detailing the state's spending of $1 million in funds received through the federal Buffer Zone Protection Program.[757] The story documented the reporter's attempts to gain access to the documents, and highlighted stories in Alaska, Washington, D.C., and Arizona in which reporters successfully sough the same records.

Other stories used DHS records to examine the growth of the so-called "no-fly" list,[758] intelligence operations that implicated antiwar groups,[759] the growth of the U.S. terror watch list,[760] the reliance on Internal Revenue Service records in terrorism investigations,[761] and a number of other issues.

751 Sara Burnett & Kara Spak, *Gas masks, a treadmill and T-shirts in suburbs, homeland security spending is all over the map*, Chicago Daily Herald, Sept. 12, 2005, 1.
752 Sara Burnett & Kara Spak, *Targeting Terror: Did Security Spending Hit The Mark?,* Chicago Herald, Sept. 12, 2005, 2.
753 *Ibid*.
754 Tim Younkman, *Terrorist attack launched wave of federal funds to Bay County*, Bay City Times, Sept. 10, 2006, A1.
755 Paul Brubaker & Tom Meagher, *Following the Money*, Bay City Times, Sept. 10, 2006, A01.
756 Bruce Golding, *Calif. more forthcoming than N.Y. with bridge inspection data*, Journal News of Westchester County, Nov. 27, 2005, 5A.
757 Eric Barton, *Secret Security; Where's Missouri's anti-terror money going? Don't ask*, Pitch Weekly, June 8, 2006, 1.
758 Eric Lichtblau, *Papers Show Confusion As Watch List Grew Quickly*, N.Y. Times, Oct. 9, 2004, A9.
759 Eric Lichtblau & Mark Mazzetti, *Military Documents Hold Tips on Antiwar Activities*, N.Y. Times, Nov. 21, 2006, A18.
760 Karen DeYoung, *Terror Database Has Quadrupled in Four Years; U.S. Watch Lists Are Drawn from Massive Clearinghouse*, Wash. Post, Mar. 25, 2007, A1.
761 Dalia Naamani-Goldman, *Anti-terrorism program mines IRS records*, L.A. Times, Jan. 15, 2007, C1.

The stories show, again and again, the effectiveness of the FOIA in generating coverage of the Department, providing evidence of productive information channels and fueling some of the more newsworthy topics that have emerged in the years since the creation of the agency.

The Department's records have been used to tell important domestic policy stories unrelated to terrorism as well. For example, several stories in the past two years have used the FOIA to examine FEMA's post-Katrina response. The Houston Chronicle, for example, cited a Mobile, Alabama Press-Register story examining FEMA spending records, finding, among other things, that the agency ordered 415,000 box lunches from a Mobile company for $6.2 million – an average of $14.85 per lunch.

Another story examined the lack of diversity among FEMA senior staff, finding, thanks to a FOIA request, that of the 19 senior executives of the agency in 2005, one was a person of color.[762] The story used the records to foster a broader discussion of the cultural issues facing persons displaced by the storm, mixing the records-driven reporting with interviews in an important feature story.

Conclusion

The risk of terrorism, and the government's response to that threat, represents one of the most compelling stories of the age. As expected, the number of articles on the DHS and its subordinate agencies increased dramatically after 9/11. Use of FOIA to generate stories related to DHS increased as well, but a broad sampling of stories from a wide variety of sources showed little or no increase as a percentage of the universe of coverage. Such a finding is supported by studies of FOIA use by reporters generally.

Despite the widespread belief that journalists are among the heaviest users of the federal Freedom of Information Act, studies have shown that the news media file far fewer FOIA requests than businesses or lawyers.[763] Examination of a large sample of journalistic coverage of the DHS and its subordinate agencies shows that where reporters have used the FOIA to produce documents from the DHS, the press has generated important work that provides meaningful scrutiny of the department's many activities. Against the backdrop of a war on two fronts and continuing terrorist threats, perhaps no agency is as important for Americans to understand, and yet the research shows that few news outlets are devoting the personnel and resources needed to fully leverage the potential of the FOIA in the homeland security arena.

This pilot study raises several questions that should form the basis of future research into coverage of the agency. Quantitative content analysis could be employed to gain a better sense of the nature of the coverage, examining such issues as tone, topic selection and the effects of coverage on audiences. The researcher has requested the FOIA logs of all DHS agencies, in a study that will better document the actual level of FOIA use by journalists and non-journalists alike. Survey research could be utilized to examine the attitudes of journalists and homeland security officials alike on matters related to information policy. Much work remains to be done to maximize information flows from DHS while addressing legitimate homeland security concerns.

762 Colleen O'Connor, *Katrina, then culture shock*, Denver Post, Sept. 25, 2005, L1.

763 Jane Kirtley, *Tapping into the government*, Communicator, Vol. L, No. 6, 31-32 (1996). *See also* The Heritage Foundation, *Few Journalists Use the Federal Freedom of Information Act: A Study by the Center for Media and Public Policy,* (2001).

Chapter 6

Terror Investigations

Synopsis
6.1 *Promises and Pitfalls in Counterterrorism Investigations* by Jarret Brachman

6.1 Promises and Pitfalls of Counterterrorism Investigations

by Jarret Brachman

The specter of terrorist attacks in the United States continues to test the government's efforts and ability to balance between bolstering liberty and ensuring order. Since 9/11/2001, both the ways in which investigative agencies in this country conduct their work on the federal, state and local levels influences, as well as the outcomes of those investigations, directly impact that delicate balancing effort.

In the United States, counterterrorism investigations generally include acquiring and pursuing leads, gathering evidence, making arrests, conducting training, collecting and sharing intelligence, and responding to terrorist related threats and incidents. The promises and pitfalls involved in each one of these processes can arise from any of three different areas: the actors involved in investigating terrorism related attacks and plots; the social, political and legal environment in which these investigations occur; and the ongoing interaction between the actors and their environments.

There have been several cases from which to draw important lessons learned for conducting future counterterrorism investigations. Some of the cases are domestic, including the Lackawanna Six, the Portland Seven, the Fort Dix Six, the North Virginia Jihad group and others. American counterterrorism cases, for whatever reason, seem to pale in comparison to international terrorism plots in terms of the acquired capabilities and level of sophistication. Some of the more concerning international terrorism investigations include the Toronto cell, the London airliner plot, the British fertilizer plot and a variety of others. Each of these investigations provide insights into the challenges of interagency coordination, timing of interdiction, dealing with overwhelming amounts of information, public misidentification of suspects, and investigating complex transnational networks.

This piece will provide an examination of previous counterterrorism investigations and discussions in order to further collective understandings about these processes and develop recommendations for avoiding pitfalls while leveraging opportunities for American counterterrorism investigators drawing heavily on analysis of actual terrorism investigations. To do this, the article will first provide a historical background of America's terrorism related struggle to combat terrorism. This section demonstrates that American thinking, policy and laws related to terrorism are constantly in flux over broad swaths of time. Importantly, it provides the necessary long-term context for any discussion on challenges of counterterrorism investigations. Second, the article teases out certain steps within the counterterrorism investigation process that have posed challenges and provided opportunities to investigators recently. Drawing on publicly available empirical evidence, the article highlights

key decision-points and consequences of a variety of counterterrorism investigations.

American History with Counterterrorism Investigations

Although one could feasibly tell the American story through the lens of the crimes that have preoccupied American attention and resources mind, it is also clear that what society considers 'criminal' behavior has evolved to some extent. Laws change. Collective attitudes morph. The 'criminal,' as most scholars who study it would attest, is an inherently social phenomenon, as clear as some behaviors seem to be. Terrorism, understood today as an act of violence perpetrated against a non-combatant target in order to make a political statement, seems to be a behavior that is considered timelessly wrong. It shocks the collective psyche. It violates the public trust. The reality is, however, that the American public has never agreed about what constitutes 'terrorism,' making it difficult for those tasked with conducting investigations on it to operate with the full public support and backing.

American history between the early 1880s and 1920s is full of stories of violence and the struggle by societies as well as governments to put that violence in context. While this era is integral to understandings of contestation over "who" and "what" should be associated with "terrorism," it is all too often glossed over in historical analyses of it. Analysis of the texts during this period reveals that social actors in this period, as in the previous historical eras examined above, contested how terrorism was understood and what the metrics were for classifying someone as fitting under its rubric.

In his 1880 dedication of the Soldier's Monument in Painesville, Ohio, President James Garfield gave what reporters subsequently described as an "eloquent tribute to the slain of the war."[1] In Garfield's brief remarks, he observed that the lessons derived from the monument include: the need to understand, "sacrifices for what we think," the "immortality of the truth," and what the American people must do to sustain itself in the face of "terrorism."[2] Terrorism, for President Garfield, meant the widespread use of violence by rogue groups domestically, particularly those thwarting reconstruction efforts in the South. As this article highlights, the American public was in no way agreed upon that understanding or any other regarding what constituted terrorism, who employed it, who suffered from it or how it ought be countered, however.

By the turn of the twentieth century, the American public had become highly attuned to developments in matters concerning anarchist violence. Anarchism, as its advocates and those sympathetic to their underlying political agenda publicly contended, was best conceived of as a protest against the rule of might, and an assertion of the rule of right. Anarchism, its apologists would argue, "believe in the rule of morality rather than in the rule of the politicians." Seeking to legitimize anarchists as a group, this author makes a strategic clarification between militants employing anarchism as legitimation for their violence, and non-violent believers in the ideology.[3]

In September of 1901, the New York Times examined a connection between the "possibility of there being a general Anarchist lot in the assassination of President McKinley and the supposed connection of Emma Goldman with the conspiracy, of another Anarchist queen more famous…Teresa Brugnoli, better known as La Bella Teresa." By linking her with Bresci, the assassin of Italian King Humbert in 1900 and describing her as being "in Europe what Emma Goldman is in America," the Times sought to help the American public, and law enforcement community by default, understand her

1 *A Speech by Gen. Garfield*, N.Y. Times, July 5, 1880, at 1.

2 *Ibid.*

3 *Two Kinds of Anarchists*, N.Y. Times, Jan. 10, 1916, at 10.

as a security threat. Quoting her as having said: "Nihilists, Fenians, Anarchists, or whatever you call yourselves, your object is the same. You can only evoke the terrorism of assassination by striking at the lives of rulers and statesmen – whether King, Emperor, Czar, or Republican President," the American public began to understand, and demand, that law enforcement do something to not only respond to terrorism in this country, but stop it before it happened. This feeling would become even further solidified in the American collective response to the violent activities perpetrated by the Ku Klux Klan.

A number of groups, most affiliated in some way with the Ku Klux Klan, arose during the early 20th century, causing significant public disturbances. Beginning as early as 1922, Governor John M. Parker and Attorney General A. V. Coco, both of Louisiana, provided President Warren Harding, Attorney General Daugherty and William J Burns, Chief of the FBI, with "an array of facts concerning the Ku Klux Klan terrorism in their State." Their goal, according to reports, was not to admit defeat. To the contrary, Governor Parker, "was emphatic in asserting that the officers of the State Administration were capable of handling the Ku Klux Klan situation as far as Louisiana was concerned and that there was no intention of appealing to the Federal Government to assume any jurisdiction." What Parker claimed he needed to rid Louisiana of the "masked organization" who perpetrated "certain outrages" and "horrifying crimes," was federal assistance to stop trans-state support of these groups.[4] Contestation over what level of government should engage in counterterrorism investigations became very heated at this time in American history.

In 1928, Ohio Attorney General, Arthur L. Gillion, filed suit against the KKK in that state. One man testified in the course of the investigation that various organizations working for the KKK carried out a "program of terror, including public whippings, burning churches, and theaters, making threats, illegal liquor raids and engaging in guerrilla warfare."[5] Further complicating matters, the investigation found that some of the violence "was closely associated with units of State government," including the Ohio National Guard.[6] In the 1930s, an organization known as "The Black Legion" began operating in the Midwestern United States. Founded by William Shepherd, the Black Legion was an offshoot organization of the Ku Klux Klan. At its peak, the group's total membership was estimated between 20,000 and 30,000, centered in Detroit, Michigan. Members were known to wear black uniforms with a skull and crossbones insignia. According to the FBI at the time, "this cult-type organization operated in the Midwest in the 1930's supposedly to protect the United States from various forms of isms."[7] They were believed to have been responsible for many murders of alleged communists and socialists, notably Earl Little, father of Black activist, Malcolm X.[8] Terrorism, by this time in American investigative history, was understood as relating to political and social groups who pursue objectives considered to be violent and discriminatory against others under the cover of darkness. The KKK was not the only counterterrorism challenge facing American investigators, though.

On 15 February 1933, President Franklin Roosevelt had just concluded a speech in Miami, Florida when, according to reporting, an "assassin fired five shots from his gun."[9] While Roosevelt went unharmed, Chicago Mayor Anton Joseph Cermak

4 *Louisiana To Fight the Klan Without Federal Aid Now,* N.Y. Times, Nov. 21, 1922, at 1.

5 *Klan Terrorism in Ohio Pictured By a Witness,* L.A. Times, Mar. 27, 1928, at 9.

6 *Ibid*.

7 See the Federal Bureau of Investigation's Freedom of Information website on historical investigations into the Black Legion at: http://foia.fbi.gov/foiaindex/blackleg.htm.

8 For more information about the Black Legion, see Peter H Amann, Vigilante fascism: The Black Legion as an American hybrid, Cambridge University Press, 1983.

9 *Assassin fires on Roosevelt; Bullet Hits Chicago Mayor,* L.A. Times, Feb. 16, 1933.

was shot and subsequently died on 6 March 1933. The perpetrator, Joseph Zangara, was described by press accounts as a brick mason who had been in Miami two months before seeking kill the President. Available historical records show no attempt by social actors to link Zangara with the notion of terrorism. To the contrary, police statements and media reporting actually portrayed the man as dimwitted and mentally unstable. For instance, one report observed, "Zangara's face was white with suppressed excitement as he answered the [interrogation] questions. His hands jerked nervously. He moved constantly, vibrantly. Between rational statements, he relapsed into irrational spasms."[10] In one statement, police reported that Zangara proclaimed, "I'd kill every President. I'd kill them all; I'd kill all the officers."[11]

While December 7, 1941 was a day that would "live in infamy" in the American mindset, it would not, however, be fit into the American public lexicon for acts of terrorism. The only association of the Pearl Harbor attack with terrorism can be found in an obscure news report about how a Japanese pilot en route to bomb Pearl Harbor with his Japanese air force compatriots ran out of gas and was forced to land on a Hawaiian island. Wandering on the Hawaiian island up to five days after the bombing of Pearl Harbor, the article goes on to write that "the story of this terrorism…is a dramatic one," where because the islanders did not yet know of the bombing, allowed the pilot to roam freely on the island. When the Japanese pilot established contact with two other Japanese sympathizers, they were able, according to the article to recover the guns from his air craft and "were in control of the village." After a fight between an island resident and the Japanese pilot, the pilot was killed.[12] The term's usage in this context does not seemed attached to, nor asserting any particular historical motif about how to understand terrorism.

The American public was also applying the label of terrorist against participants of the Japanese by the early 1940s. In 1942, the FBI was aggressively rounding up "known and suspected members of the toughest alien Japanese group in San Francisco."[13] The raids were said to have been based on documentary evidence seized in previous raids on Japanese secret societies, that the local group was a "front" for the ruthless and dread Black Dragon Society, most nationalistic and terroristic of all Japanese secret bodies. Nat J.L. Pieper, Northern California FBI chief who directed the roundups, said some of the Japanese already in custody had admitted the secret nature of the local society. Mr. Pieper also declared "proof of the organization's intense nationalistic program, and direction under the Black Dragon Society, has been found." And in public discussions about the death of Mitsuru Toyama, referred to widely as a "terrorist leader" and "unofficial emperor" of Japan, publics contested that his lead of the Black Dragon Society, a group that was notorious for targeted assassinations as well as known as a group of "drug peddlers, brothel keepers, smugglers and swindlers that swarmed into China from Japan to take advantage of the turmoil during the Chinese revolution.[14]

The onset of the Cold War introduced a new enemy within American popular discourse, communists. President Truman used the term terrorism to help generate Congressional and public support for massive U.S. assistance to Greece.

> The very existence of the Greek state is today threatened by the terrorist activities of several thousand armed men, led by Communists, who defy the government's authority at a number of points, particularly along the northern boundaries. A Commission appointed by the United Nations Security Council is at present investigating dis-

10 *Ibid*.
11 *Ibid*.
12 The Sheboygan Press (WI), Jan. 2, 1942, at 15.
13 *FBI Raids Jap Terrorists,* San Francisco News, Mar. 31, 1942.
14 *Toyama of Japan, Terrorist Leader*, N.Y. Times, Oct. 6, 1944, at 23.

> turbed conditions in northern Greece and alleged border violations along the frontier between Greece on the one hand and Albania, Bulgaria, and Yugoslavia on the other. Meanwhile, the Greek Government is unable to cope with the situation. The Greek army is small and poorly equipped. It needs supplies and equipment if it is to restore the authority of the government throughout Greek territory. Greece must have assistance if it is to become a self-supporting and self-respecting democracy.[15]

Using the term terrorism to cast a negative light on the communist insurgents challenging the Greek government, President Truman was launching what would be the first of a fifty year policy of supporting democracy against the forces of communism worldwide. Interestingly, the first justification of the Cold War is rooted in Truman's argument that these forces are terrorist in nature. The term would continue to be used and contested as public actors sought to justify a shift in U.S. policy in the establishment of the CIA.

In the initial discussions of establishing the Central Intelligence Agency, Major General William J. Donovan, director of the Office of Strategic Services (OSS), proposed what he envisioned as an organization very different from the "terroristic character of a Gestapo" – which the CIA, in its earliest inception, was being compared to in certain Washington circles. On the contrary, according to the article, what would be the future organization's "personnel would be without police authority over United States citizens and would operate only from the point of view of information and interpretation." According to the article, "control of this organization is vested with Congress. Congress could therefore prevent its being turned into an agency for terrorism by limiting its appropriation."[16]

At the 1972 Summer Olympics in Munich, Germany, the Palestinian group, Black September, a group designated as terrorists by the U.S. government, took the Israeli Olympic team hostage, leading to the deaths of 11 Israeli athletes, five of the eight kidnappers, and one German police officer.[17] The group demanded the release and safe passage to Egypt of 234 Palestinians jailed in Israel, and an additional two in German prisons. Israel's response was immediate and absolute: there would be no negotiation. The German authorities, under the leadership of Chancellor Willy Brandt rejected Israel's offer to send an Israeli special forces unit to Germany. The German police who took part in the operation had no special training in hostage rescue operations.

After this incident, publics significantly questioned their governments about security preparedness. Counterterrorism moved from the negative conceptions that it carried with it as a legacy from Algeria and British contexts, and increasingly became seen as something governments needed to provide for their countries. And governments began to realize that there were stratifications across their ability to fight hijackers and kidnappers. The legacy of the 1972 Olympics would go on to inform how every government thought about the worst-case scenario when they hosted future games. It also became a standard recollection for any discussion about security preparedness within American media reports from that point forward.

Leading up the 1984 Olympics public contestation over the social fact of terrorism was intense. By this time, federal policymakers had fully embraced the idea that terrorism was a something that could be measured, tracked and fought; academics embraced the notion that terrorism could be studied, parsed, categorized and discussed historically; and publics had embraced the idea that there

15 Harry S. Truman, Address Before a Joint Session of Congress, (Mar. 12, 1947),*available at* http://www.yale.edu/lawweb/avalon/trudoc.htm. (last visited May 24, 2004).

16 *Donovan Upheld On Peace Spy Plan*, N.Y. Times, Feb. 13, 1945, at 14.

17 *See* "One Day in September: The Full Story of the 1972 Munich Olympics Massacre and the Israeli revenge operation," (New York: Simon Reeve, 2000).

were actors known as terrorists who intended to kill them for any number of reasons. The Olympics held in Los Angeles, California in 1984 led to some novel discussions and actions by the U.S. government regarding terrorism. In the lead up to the event, Los Angeles Police Chief, Daryl Gates, took a trip to West Germany, Israel, Britain and France where he "consulted at length with security authorities" about preventing terrorism. The Los Angeles police then brought in Shaul Rosolio, a former Israeli chief police commissioner, where he "held private meetings for several days with law enforcement and Olympics security officers." Intelligence sources, according to reports, had been reflecting possible violence at the games spurned from either conflict in Central America or anti-Turkish sentiment.[18] In a controversial and unprecedented move, the FBI "did what no other counterterrorist team in the world has done: showcased its capability to rescue hostages with minimum loss of life" by running a high-profile hostage-rescue scenario. FBI Assistant Director, O.B. Revell noted that the simulation was designed to "demonstrate to anyone who might engage in terrorist acts that we have this capability."[19] One of the most concerning threats for Americans leading up to the 1984 Olympics were Armenian groups. The FBI Director singled out the Armenins as a principal threat, a statement that further strained the relationship between law enforcement officials and the Armenian community in the United States, according to media reports. The director of a for-profit terrorism research center argued that Armenian terrorism "is not tremendously unlike the Italian community in organized crime cases years ago," particularly in how the "law-abiding Italian community resisted cooperating with us because of the feeling that they shouldn't talk about their own."[20]

An unnamed intelligence official interviewed by The New York Times contested, "gathering intelligence about terrorism, particularly trying to penetrate terrorist groups, is considered one of the toughest jobs in the intelligence business."[21] Trying to free himself and his organization from the mounting public pressure about what was needed to fight terrorism, this official represents the type of defensive relationship policymakers began to find themselves in during the 1980s, seeking to find the precarious middle ground between over-reacting and under-performing. The Defense Department faced a similarly difficult task. In December, 1983, for instance, reports highlighted how the Department of Defense, "in response to criticism that the United States military is not equipped to fight terrorists, [was] hastily preparing proposals for confronting the problem for review by Defense Secretary Caspar W. Weinberger," department officials announced. While the DOD was actively asserting its need to prepare to counter terrorism "anti-terrorism experts in universities, research institutes and consulting firms across the country," media reports contested the departments' statements, contending that the military's "sudden interest in terrorism would fade."[22]

The FBI was not free from such public demands either. They made particular efforts to enhance both their ability to combat terrorism as well as public visibility of those efforts. For instance, they announced the development of a computer system for analyzing intelligence, where "tidbits from around the country and the world are fed into computers and go to our analysts for investigative guidance…the computer tracks movements and associations. It relates incidents in one part of the country with another through a license plate or similarity of names," said an FBI official.

18 Kenneth Reich, *Gates, Terrorism Experts Meet About Olympics*, L.A. Times, June 7, 1983, at SD_A3.

19 Evan Maxwell & Roland Ostrow, *Displays Arsenal For Olympics*, L.A. Times, Mar. 10, 1984, at A25.

20 Evan Maxwell, *Fear of Armenian Terrorism at Games Spurs Both Anger, Calls for Cooperation*, L.A. Times, July 28, 1984, at A1.

21 *Intelligence: Too Much Information, Too Little Evaluation*, N.Y. Times, Dec. 11, 1983, at 51.

22 Joel Brinkley, *Pentagon Hastily Drafts Measures on Terrorism*, N.Y. Times, Dec. 30, 1983.

Despite the fact that the media heralded the "dramatic drop in the number of major terrorist incidents" since the bombing of the TWA Flight 840 and of the American embassy in Kuwait, some argued as fact that "the Reagan administration's anti-terrorism effort is almost universally regarded as a failure." This theme was reinforced by a book on terrorism called "Best Laid Plans: The Inside Story of America's War Against Terrorism," written by two investigate journalists.[23] In the book, they seek to demonstrate the complexities of responding to terrorism as the president. Additionally, they argue that terrorism experts are unrelenting, criticizing a president for being too harsh one day in dealing with terrorists and too soft the next."[24]

Others, including the presidents themselves, sought to argue that the President needs to be freed from conventional constraints in fighting terrorism because it is an unconventional threat. One article highlights how both Presidents Carter and Reagan "challenged the legality of the Vietnam-era War Powers Resolution, and asserted that the president needn't notify Congress of every covert operation – particularly if he believes that such notification might jeopardize lives." A Deputy Assistant Attorney General in the Reagan Administration publicly asserted with regards to this point that "Congress has got to make it clear that the rules don't apply to [fighting] terrorism."[25]

In the aftermath of the hijacking of a Kuwaiti Airways 747 for 16 days, the hostage-takers made demands to release colleagues from prison. The Kuwait government refused their demands, which elicited praise from many American actors who argued, for example, that "the forces opposing global terrorism are the stronger this week for Kuwait's firm decision not to give in to hijacker demands."[26] President Reagan condemned another bombing, this time against the U.S. Embassy in Beirut, saying, despite continuing threats from "the worldwide terrorist movement," the United States "can't crawl in a hole some place and stop performing."[27] In April 1984, President Reagan signed a secret directive described by officials as a broad charter for "taking the offensive" against terrorism.[28] But in the aftermath of the Beirut embassy bombings, many began criticizing President Reagan for not living up to his comments a week after his inauguration where he promised America "swift and effective retribution" for terrorist acts. In an effort to defend Reagan, Secretary of State George Schultz argued that terrorism "is really a form of warfare" and therefore needed to be handled cautiously, particularly when hostages were involved.[29]

In 1984, the Christian Science Monitor contended that "as the seizure of a Kuwaiti jetliner this week shows, skyjacking has become much less a mode of transportation than a means to terrorist ends."[30] Attempts like these by social actors to delineate key moments in time or critical junctures are those that denote a change in the dominant trajectory. In this case, it was the fact that hijackers used planes to get themselves to countries they otherwise might not have been able to – Cuba and Iran were particularly common destinations – as well as a means to publicize their political events.

The Reagan Administration, moving forward with plans for action against international terrorism, considered whether to exempt punitive raids against terrorists from its policy against assassina-

23 David Brooks, *No Way to Win Anti-Terrorism Game*, Wall St. J., Sept. 2, 1988, at 11.
24 *Ibid*.
25 Robert S. Greenberger, *Free the Presidency to Fight Terror*, Wall St. J., Dec. 19, 1985, at 28.
26 *Not a Victory for Terrorism*, Christian Science Monitor, Apr. 22, 1988, at 15.
27 John M. Goshko, *Reagan Decries Attack, Stays Firm on Terrorism*, Wash. Post, Sept. 21, 1984, at A1.
28 *Ibid*.
29 Brad Knickerbocker, *US Officials Search for Practical Ways to Combat Terrorism*, Christian Science Monitor, Oct. 18, 1984, at 1.
30 Peter Grier, *Hijacking is Down, But Aims Have Changed*, Christian Science Monitor, Dec. 7, 1984, at 1.

tions, officials said in 1985. Toward that end, State Department lawyers had apparently been examining centuries-old piracy laws to see whether they offer legal justification for attacking or capturing terrorists. A senior White House official contested the "war whooping in the media and the Congress about what we ought to do in Beirut," instead the official argued that "most of what is called for in the fight against terrorism is just painstaking police work, on a global scale."[31]

This reassessment included looking to the examples of the European government who, in 1986, began authorizing new surveillance and identification polices. The French Interior Minister asserted a new framework for governments and societies to understand counterterrorism by saying, "It's time to start terrorizing the terrorists."[32] Contrary to the American strategy to place pressure on nations perceived as sponsoring terrorism, Europeans argued that their efforts monitoring publics had been paying off. The plan, including the "possibility of an ID check, limits the terrorist's sense of freedom to act," one French government official argued. "The terrorist will know he can't so easily hide behind his anonymity," said another.[33] The U.S. government seemed less enthusiastic about taking more aggressive efforts domestically, including anything that could be construed as limiting civil liberties. Director of the Federal Protection and Safety Division of the General Services Administration contended, "If we shut [public buildings and monuments] down, then that is what the terrorists want us to do, to shut down the operations of the government." Free and unconstrained access to "symbols of a free society," should not be changed, he argued.[34]

31 Doyle McManus, *Assassination Ban May Not Apply in Anti-Terror Raids*, L.A. Times, July 13, 1985, at 1.

32 Roger Ricklefs, *Europe Getting Tougher With Terrorists*, Wall St. J., May 28, 1986, at 38.

33 *Ibid*.

34 Warren Richey, *Security vs. Openness in the U.S. Capital*, Christian Science Monitor, May 6, 1986, at 3.

The Modern History of Counterterrorism Investigations

U.S. Government understandings of terrorism continued to morph through the 1990s, in large part due to the changes occurring around the world in both thinking about and combating terrorism. For instance, in late 1989, an unofficial meeting of United States and Soviet terrorism experts produced "ambitious proposals for joint action between the superpowers." The former CIA Deputy Director of Central Intelligence, Ray Cline, argued that "it is clear to me that in the back of their minds the Soviets now see terrorism is a threat to the Soviet Union, not just the United States." Cline went on to say that the Soviets "would like to get on the side of the angels on this one."[35] The British Government drastically altered their counterterrorism infrastructure in 1992 by unleashing their intelligence agency, MI5, against terrorism. Britain's Home Secretary told the British House of Commons that "MI5, now virtually free of its commitment to fighting communist regimes, was taking over from the Metropolitan Police (Scotland Yard) the 'lead responsibility' for countering Irish terrorism in Britain." The decision, according to an unnamed senior British official, was triggered by a April 1992 Irish Republican Army bomb attack in London's financial district that ripped through an entire city block, disrupting the operations of dozens of banks and other financial institutions.[36]

Under President Bill Clinton, the United States continued to face attacks that publics and the government construed as being terrorism. President Clinton had been in office for just 38 days when a group of Islamic radicals bombed the World Trade Center, killing six people and injuring more than 1,000. Public reaction did not immediately attribute the explosions to terrorism. The new president's reaction seemed to many, almost disengaged. He

35 Scott Armstrong, *US-Soviet Panel Drafts Antiterror Plan*, Christian Science Monitor, Oct. 2, 1989, at 8.

36 Alexander MacLeod, *British Spy-Catchers Set Sights on Domestic Terrorism*, Christian Science Monitor, May 13, 1992, at 6.

pleaded with the American people and the people of New York to "keep your courage up and go on about your lives. I would discourage the American people from overreacting to this." Clinton assured Americans that he had put forth "the full, full resources of the federal law enforcement agencies - all kinds of agencies, all kinds of access to information - at the service of those who are trying to figure out who did this and why." He also said he would implement a policy of "continued monitoring." Clinton said the United States was "absolutely determined to oppose the cowardly cruelty of terrorists, wherever we can." Federal law-enforcement authorities in New York concluded that Sheik Omar Abdel Rahman, the radical Egyptian cleric seen widely as providing ideological inspiration to the bombers, "knew details of the plot to detonate bombs across the city and assassinate several officials but were waved off of arresting him at the last minute by the Clinton Administration, Government officials said today."[37] According to the Administration, they decided to allow him to remain at-large because they had an ongoing electronic surveillance on him and thought he was more useful as a source into the murky world of Islamist extremism than he would be as a tactical source or legal boon.[38]

In preparation for the first anniversary of the 1993 World Trade Center bombing, the New York Police Department "sent bomb-sniffing dogs to survey landmarks like the Empire State Building, the Statue of Liberty and other likely targets of terrorism. The dogs hunted inside but made a special survey of the perimeters, part as a show, said John F. Timoney, the chief of police." He clarified the act as a way to "let them know whoever 'they' are, that we haven't forgotten."[39] From the start, many saw President Clinton as approaching the investigation as a law-enforcement issue. In doing so, he limited the types of resources that could be brought to bear on the attacks, particularly that of the intelligence agencies. For example, the evidence gathered by FBI agents and prosecutors came under the protection of laws mandating grand-jury secrecy—which meant that the law-enforcement side of the investigation could not tell the intelligence side of the investigation what was going on. "Nobody outside the prosecutorial team and maybe the FBI had access," says James Woolsey, who was CIA director at the time. "It was all under grand-jury secrecy."

Another problem with Clinton's decision to assign the investigation exclusively to law enforcement was that law enforcement in the new administration was in turmoil. When the bomb went off, Clinton did not have a confirmed attorney general; Janet Reno was awaiting Senate approval. The bombing barely came up at Reno's Senate hearings. The focus of much of the media's coverage of the U.S. Government's counterterrorism efforts following the 1995 Oklahoma City bombing were focused on defending against domestically-rooted groups. While federal and state investigators focused increasing attention on movements of the far right "white supremacists and paramilitary groups in the wake of the bombing, many of the legal powers they sought in the emotional aftermath of the blast to aid the gathering of evidence have not been enacted."[40] And since that attack, as this article identifies, "arrests on terrorist charges have been made nationwide, and federal agents have confiscated truckloads of weapons, including machine guns and pipe bombs, ammunition, explosives of every description, chemicals and deadly poisons."[41]

In his address to honor the victims of the Oklahoma City bombing, President Clinton vowed to petition Congress for broad new powers to fight

37 David Johnston, *Sheik Was Aware Of Bombing Plot, U.S. Officials Say*, N.Y. Times, June 28, 1993, at A1.
38 *Ibid*.
39 Matthew L Wald, *How Does the World Look Through the Eyes of Aspiring Terrorists*, N.Y. Times, Mar. 6, 1994, at E3.
40 John Kifner & Jo Thomas, *Singular Difficulty in Stopping Terrorism: Lone Fanatics Can Still Slip Through Web of Tougher Surveillance*, N.Y. Times, Jan. 18, 1998, at 24.
41 *Ibid*.

terrorism, including "creation of a domestic counterterrorism center headed by the Federal Bureau of Investigation" and expanded surveillance capacity ascribed to the federal authorities. Clinton ordered a review of security at all federal buildings and renewed the U.S. Government's commitment to fighting terrorism both domestically and abroad. According to the article, Clinton's proposals "would reverse a two-decade trend away from Federal surveillance of government critics, which was curtailed after disclosures of widespread abuses and harassment of civil rights and antiwar protesters in the 1960's and 70's." The article cites Philip S. Gutis, media relations director for the American Civil Liberties Union, as saying that "we are concerned about an overreaction that would threaten to sweep away the constitutional principles that have shaped our society and remain at the core of our liberty."[42]

And then on June 25, 1996, a truck bomb exploded outside the Khobar Towers barracks in Dhahran, Saudi Arabia, killing 19 American soldiers and wounding hundreds more. President Clinton vowed to bring the killers to justice. "The cowards who committed this murderous act must not go unpunished," he said angrily. "Let me say again: We will pursue this. America takes care of our own. Those who did it must not go unpunished." The next day, Clinton reiterated that, "we will not rest in our efforts to find who is responsible for this outrage, to pursue them, and to punish them." Calling the attacks an "outrage" rekindled public memories of previous terrorism discourse.

In an editorial, the author writes that "the Government has the power under existing law to crack terrorist groups. If the FBI and other agencies need more money or manpower, the White House and Congress should provide it – but not a license to interpret the Constitution as they see fit."[43] The FBI at this time "opened a high-technology, $20 million operations center at its headquarters this week to give officials better tools to manage as many as five crises at once. The efforts by FBI officials in 1996 to handle three big cases at the same time – the Olympic bombing in Atlanta, the explosion of T.W.A. Flight 800 off Long Island, and the Khobar Towers truck-bombing in Saudi Arabia – made it clear that a new center was necessary." The article continues, "the Bureau's fastest growing component, its Counterterrorism Center, is arrayed in the offices around the high-technology center – as is its violent crime unit, which handles domestic attacks."[44] Clinton's proposals would cost $1.5 billion over five years, adding around 1,000 new Federal agents, and importantly, seek to amend the landmark Posse Comitatus Act of 1878 to allow military experts to help civilian authorities investigate crimes involving 'weapons of mass destruction.'"[45] But FBI Director Louis Freeh contested at a Senate oversight hearing that "it is clear that we were told to investigate domestic terrorism differently from foreign terrorists," indicating bureaucratic confusion with regards to the priorities and instrumentalities for handling various types of attacks based on definition.[46]

In response to political fire from House Speaker Newt Gingrich, President Clinton stated that "nothing can justify turning this bill into a political football…we have kept politics completely out of our fight against terrorism. We kept it out of our mourning. We kept it out of our law enforcement efforts…" The bill at the time planned to create a 'Domestic Counterterrorism Center' counterpart to the CIA's already existing Counterterrorism Center which focused on foreign threats but prohibited by law from spying on American citizens.[47] Reports highlighted how Congress, ac-

42 Todd S. Purdum, *Ease Restrictions: Liberties Groups Worry about 'Overreaction' to Bombing Attack*, N.Y. Times, Apr. 24, 1995, at A1.

43 *Don't Legislate in Haste*, N.Y. Times, Apr. 25, 1995, at A22.

44 *Crisis Center Is Expanded and Updated By the F.B.I.*, N.Y Times, Nov. 22, 1998, at 39.

45 Todd S. Purdum, *Clinton Seeks More Anti-Terrorism Measures*, N.Y. Times, Apr. 27, 1995, at A1.

46 Francis X. Clines, *F.B.I. Chief Seeks Orders For Inquiries*, N.Y. Times, Apr. 28, 1995, at A25.

47 Tim Weiner, *Clinton Urges Fast Action on Terror-*

cording to Gingrich, was, "reluctant to give the Federal Bureau of Investigation more authority to fight terrorism because lawmakers felt the Bureau had mishandled the investigation of files given to the White House." The "rushed effort to pass new antiterrorism legislation last week before Congress left for its August recess failed when Senate Democrats refused to accept a House-passed version that left out two White House proposals."[48]

The 1998 Embassy bombings triggered discussion about "coordinating an effort with European and African nations to roll up the terrorist networks of Osama bin Laden." United States officials said that they believe that the question is not "whether Mr. Bin Laden will strike again, but when." Reports sought to clarify that "Mr. Bin Laden has been a focus of attention at the CIA, Counterterrorism Center for years, and he has been identified in a Presidential finding that authorizes covert action to combat international terrorism."[49] Gerecht, a former CIA Middle Eastern specialist, begins articulating that "the guiding tenet of terrorism is to do a lot with a little. From the Assassins in the Middle Ages to Osama bin Laden, terrorists have aimed at targets that will help magnify their real strength." This editorial, pointing to that component of the terrorist method, asks why the Clinton administration authorized the issuance of State Department bulletins warning American citizens of potential attacks during the holiday season. Arguing that "this was free advertising for anti-American terrorists, feeding perceptions that the Middle East's holy warriors have scared the United States."[50] Gerecht states that "counterterrorism operations in the Central Intelligence Agency – in theory the cutting edge of our effort – aren't in good shape. Bloated, intellectually undernourished, and linguistically bereft, the CIA Counterterrorism Center generates more heat in Washington than it does overseas….The Clinton Administration should understand that neither United States citizens nor foreign intelligence services are helped by Washington periodically screaming 'fire.'"

Secretary of State Madeleine Albright sought to put things in perspective, observing, "this is a confrontation not so much of armies as of values and emotions; of reason versus hate; of faith versus fear. It is not as much a clash between cultures or civilizations; it is a clash between civilization itself and anarchy -- between the rule of law and no rules at all. In this struggle, our adversaries are likely to avoid traditional battlefield situations because there, American dominance is well established. We must be concerned, instead, by weapons of mass destruction and by the cowardly instruments of sabotage and hidden bombs. These unconventional threats endanger not only our armed forces, but all Americans and America's friends everywhere. We must understand that this confrontation is long term. It doesn't lend itself to quick victories. To prevail we must summon our courage, and we must equip ourselves with a full range of foreign policy tools. Our armed forces must remain the best led, best trained, best equipped and most respected in the world."[51]

When border police arrested a man last December for smuggling bomb parts from Canada, the authorities suspected a plot to turn the millennial New Year celebration into a terrorist fiasco and the Customs Bureau immediately reinforced security along the border. Amid intense publicity, President Clinton asked Congress to increase spending by $300 million for efforts to counter international and domestic terrorism. A senior Clinton administration official was quoted as saying, "In each of the last two years we have made a set of concentrated proposals involving counterterrorism and threats to critical infrastructure, and

ism Bill, N.Y. Times, May 9, 1995, at A18.

48 *F.B.I. Blamed For Lack of Bill on Terrorism*, N.Y. Times, Aug. 5, 1996, at A18.

49 James Risen, *U.S. Directs International Drive on Bin Laden Networks*, N.Y. Times, Sept. 25, 1998, at A3.

50 Reuel Marc Gerecht, *Alarmism Abets the Terrorists*, N.Y. Times, Dec. 23, 1999, at A29.

51 Secretary of State Madeleine K. Albright, Remarks to the American Legion Convention, New Orleans, Louisiana (September 9, 1998). As released by the Office of the Spokesman U.S. Department of State.

Congress has just plain not caught up…In a couple of cases which we think are really important, they really haven't put their money where their mouths are." The article cites Congress' failure to fund any of the $24 million requested by the Clinton administration to expand the number of JTTF offices around the country. According to the article, "some experts say delays are exacerbated because fighting terrorism is assigned to myriad federal agencies, whose spending is controlled by a variety of committees and laws."[52]

Interagency Cooperation Today

Before 9/11, international law enforcement cooperation specifically on the issue of terrorism was case-by-case. Consider, for instance, that Latvian Interior Minister Mareks Seglins, State Police chief and Security Police chief held talks in September 2000 with the FBI director, Louis Freeh, in Riga where they agreed on additional assistance by the FBI in investigating the [two] explosions at a supermarket in Riga in mid-August through forensic tests and investigation methodologies. Reksna said that most of the required forensic tests in the Centers department store blast case had already been carried out but a great amount of materials had to be screened again and again to find as much evidence as possible. Director Freeh said that crimes such as the department store blasts were very difficult to solve in general and the public support was vital. Cooperation in dealing with the most important problems, like drug trafficking and computer crimes, was also discussed at the talks with the FBI head, the Latvian State Police chief said.[53]

Since 9/11, a variety of regional and international partnerships have emerged centered on improving counterterrorism investigations. Old security allies have grown closer, like the U.S., Canada and Britain. New security partners have emerged, like Pakistan and Saudi Arabia. With each successful venture into international counterrorism investigations, the precedent and practicality grows stronger and more enduring. Consider the 2002 and 2004 bombings against popular tourist targets in Bali, Indonesia that reinforced the importance for countries in that part of the world of developing sustainable working relationships with regional partners In the past five years, that region has seen a strengthened commitment from law enforcement agencies to work collaboratively.

Joint terrorism investigations have helped in the systematic dismantling of the Jemaah Islamiah network, with the Indonesian National Police playing an instrumental role in the arrest of hundreds of suspected terrorists, including senior JI figures. The co-operation between Indonesian and Australian authorities has also led to advances in forensic and bomb data capabilities that are being used to track terrorists and respond to terrorist incidents across the world. For example, the disaster victim identification protocols formulated during the investigation into the first Bali bombings have been adopted as the international standard. According to some reports, the Jakarta Centre for Law Enforcement is a regional training and educational facility that has been operating for three years and has educated approximately 2,000 police and security students from across the region who gain skills in how to combat all forms of transnational crime and terrorism.

India has begun cooperating on counterterrorism, albeit in a very selective way, with its neighbor Pakistan. The Indian National Security Adviser, M. K. Narayanan has said that he has "pretty good evidence" of the Pakistani ISI's [Inter-Services Intelligence's] involvement in the Mumbai that blasts would be shared with Pakistan after "certain legal issues" are clarified and hoped this would be done before the Foreign Secretaries of the two countries meet in New Delhi on this issue. "If the anti-terrorism mechanism goes forward and we see there is a great deal of cooperation forthcoming from Paki-

52 Steven A. Holmes, *Antiterrorism Spending Falls Short, Administration Says*, N.Y. Times, July 30, 2000, at 18.

53 Tallin Baltic News Service, Sept. 18, 2000.

stan and there is a great deal of comfort between India and Pakistan, then maybe we could (share intelligence)," Narayanan said on the "Devil's Advocate" programme on CNN-IBN when asked if intelligence would be shared with Pakistan. "That (sharing intelligence) is our ultimate hope. But that's at a much later stage," he added. Narayanan said the mechanism would mostly deal with ongoing investigations and sharing of information and could look into issues like money laundering. The counterterrorism coordination mechanism will be headed by a special secretary or additional secretary, which is aimed at putting Pakistan "on the spot" and that it will be given a "fair opportunity" before India decides whether the mechanism is working or not. "If every time we give them information, we get a negative answer, then we know the mechanism is not working and we have to see what to do," he said.[54]

Another important joint counterterrorism investigative effort is that between Kazakhstan and Uzbekistan, who established that relationship by investigating the terror attacks in Uzbekistan in spring and summer 2007, Kazakh Ambassador Tleukhan Kabdrakhmanov told a news conference in Tashkent. "A joint Uzbek-Kazakh team is looking for the masterminds behind the terror attacks in Uzbekistan," he said. The team was set up following a series of attacks in the capital and the Tashkent and Bukhara regions in March and April of 2007, which resulted in the deaths of 47 people, including the 33, and injuring 35. The joint investigative team is also looking for the organizers of the Tashkent bombing attacks outside the Prosecutor General's Office and the U.S. and Israeli Embassies on July 30, 2007. The prosecution services, the Interior Ministries and special services of the two countries are maintaining close cooperation on these attacks in particular working in Jambul region and moving to the South Kazakhstan region.[55]

Spain and France too have made plans to establish a joint police teams in order to investigate international terrorist networks, the head of Spain's police and civil guard, Joan Mesquida, told reporters in October 2007. "We want to set up joint investigation teams aimed at dismantling international terrorism networks and their financing," he told a joint news conference with his visiting French counterpart Frederic Pechenard.[56] "We want to move forward with the analysis of the use of the Internet as an important tool for proselytizing for this type of terrorism," he added. The teams will be modeled on the cooperation that already exist between Madrid and Paris in the fight against the armed Basque separatist group ETA. Of the 354 members or supporters of ETA who have been arrested over the past four years, 138 -- nearly 40 percent -- were detained in France which has traditionally been used as a rear base by the group, said Mesquida.[57]

Perhaps more than any other country, however, the United States has made interagency coordination and joint investigations a priority since al-Qa`ida's attacks of 9/11 and the subsequent 9/11 Commission Report recommending a number of steps to increase integration within the American counterterrorism community. Since the establishement of the agency now charged with the mandate of fostering interagency coordination, sharing and integration, the National Counterterrorism Center (NCTC) has made important strides.

Questions of When to Move

At some point during the course of an investigation law enforcement needs to make the decision to intervene in order to thwart an impending disaster. Investigators must decide between their ability to acquire enough evidence to ensure successful prosecution and prevention of a cell from going

54 New Delhi PTI News Agency in English Oct. 22, 2006, "India To Share Intelligence With Pak Only at a Later Stage;" interview referred to in the report to be telecast by CNN-IBN at 1500 GMT Oct. 22, 2006.

55 Moscow Interfax in English 1227 GMT, Aug. 24, 2004.

56 Oct. 16, 2007, "French Police To Set Up Joint Terrorism Investigation Teams" -- AFP headline.

57 *Ibid*.

operational. Premature interdiction can mean that prosecutions are protracted or failed because they are forced to rely more on circumstantial evidence.

Police in Victoria and New South Wales, Australia, for instance had recently identified and wrapped up a cell for stockpiling explosive chemicals and that authorities under the logic that they were preempting what they believed to be an imminent attack, although they said they were unaware of the exact target. At 0230 the morning of the police raids, hundreds of security officers descended on Sydney and Melbourne. Supported by heavily armed counter-terrorism units, and with helicopters hovering overhead, hundreds of officers searched 15 properties in New South Wales. Police Commissioner Ken Moroney announced that in New South Wales, six persons, five of them Australian, were arrested in the raids after a sixteen-month counterterrorism investigation. Named Operation Pandanus, the investigation followed the suspects' movements and established the links between Sydney and Melbourne. At some point, however, investigators determined that they could no longer wait and had to interdict in order to prevent a terrorist act from occurring. This decision would lead to significant debate between senior law enforcement officials who argued "the intelligence that we've been receiving has been consistent back over the last couple of years," and senior political officials, including the Prime Minister, who pointed to specific and new intelligence that led them to issue the order to wrap up the cell.[58] The ongoing tension between law enforcement and civilian policymakers regarding the timing of moving from the investigation phase to the arrest and prosecution phase occurs in nearly every single case.

In a more well-known instance of this debate playing out publicly, British intelligence services were widely criticized for failing to monitor and disrupt planning for the July 2005, transit bombings in London. The Intelligence and Security Committee of Parliament - in the most authoritative report on British intelligence weaknesses - argued that the British agencies should have paid greater attention to the threat from homegrown terrorism and should have posted a more watchful eye on the movements of terrorist suspects between Britain and Pakistan.

Two years later, another debate would ensue, this time whether British and American investigators jumped too quickly on a cell that was not necessarily in the final stages of operationalizing their plot to destroy a dozen trans-Atlantic airliners using liquid explosives. In this case, Rashid Rauf, a lead suspect, was being watched by international security agencies after the British government received a tip that he was in Pakistan: "He has been staying here for quite some time and has been under strict surveillance since then," a Pakistani intelligence source said. "His calls to Britain and internet communications have been under surveillance that helped in revealing the plot." Britain's intelligence services had been watching some of the suspects since the informant tipped them off in December 2005. Following Rauf's arrest, one of his associates is understood to have phoned the UK urging those alleged to have been involved in the plot to speed up their plans. The call was intercepted by British intelligence and triggered the decision to arrest the suspects. It was this decision, however, within the course of the investigation that has opened significant debate. A careful reading of open source reporting seems to suggest that the United States government pushed the British government to arrest Rashid Rauf before they were prepared to, even possibly threatening to "render" him or pressure the Pakistani government to arrest him. According to some reports, British security was concerned that Rauf be taken into custody "in circumstances where there was due process," according to one official, so that he could be tried in British courts.

58 Melbourne Radio (Australia), Nov. 08, 2005, Excerpt from ABC Radio National's "The World Today" programme.

The American government would then, according to some reports, pressure the British government to move on arresting the entire cell shortly thereafter, again earlier than the British government was prepared. British officials knowledgeable about the case said British police were planning to continue to run surveillance for at least another week to try to obtain more evidence, while American officials pressured them to arrest the suspects sooner. The officials spoke on condition of anonymity due to the sensitivity of the case. In contrast to previous reports, one senior British official suggested an attack was not imminent, saying the suspects had not yet purchased any airline tickets. In fact, according to some officials, several members of the attack team had not yet obtained passports.[59]

On June 2, 2006, a Canadian police tactical unit burst into the family's Mississauga home with weapons drawn, a scene repeated around the Toronto area that day when over 500 law enforcement and security personnel broke-up a suspected terrorist building and Toronto offices of the Canadian Security Intelligence Service. Charges against the group include participating in or contributing to the activity of a terrorist group, including training and recruitment; providing or making available property for cell that they had been investigating for several years. Thirteen men and four youths were arrested in this massive police sweep against men alleged to be part of an Al-Qa'ida-inspired cell plotting to bomb several targets such as the Toronto Stock Exchange terrorist purposes; and the commission of indictable offences, including firearms and explosives offenses, for the benefit of or in association with a terrorist group. According to the Crown's synopsis, which was made public by a defense lawyer, the alleged terror plot was dubbed Operation Badr.

It included storming the Parliament Buildings and beheading politicians until their demands were met that Canada pull out of Afghanistan and release Muslim prisoners from Canadian jails. By mid-March 2006, the group had reportedly split after Ahmad and Amara disagreed on tactics - the former is alleged to have preferred the idea of shooting sprees, whereas the latter wanted to conduct truck bombings. Plans were underway by the spring to procure ammonium nitrate, a fertilizer that can be used to make bombs, according to the synopsis. The Canadian decision to interrupt the cell at that time was justified as a result of two major themes: investigators believed that they had enough evidence to support a successful prosecution and that they could no longer afford to follow the cell's plotting without threatening the security of Canada.

New Trends: Intelligence-Driven Investigations

Counterterrorism operations depend for their effectiveness on local communities that must share repugnance over terrorist ideology and methods, and be willing to trust and work with the authorities. It can be a tall order, especially for Muslim communities that feel unfairly targeted and blamed. A working relationship between communities that might harbor jihadists, local police, and intelligence agencies becomes especially important in cases of homegrown terrorism. MI5 and the British police have been involved in a lengthy surveillance of some of the suspects, dating back months. Security officials sprung their trap when they obtained evidence that planning for the airline bombings was moving forward, and that there was a threat the alleged plot might be exposed in public, driving the perpetrators underground and out of reach.

A publication ban prohibits reporting any of the court evidence and is a common tool used in the United Kingdom to mitigate the bias of a prospective jury pool. In this case, before the ban was established, significant levels of information were publicly released. It is alleged, for instance, that in 2004 Canada's spy service, CSIS, began moni-

59 U.S., U.K. at odds over timing of arrests, By Aram Roston, Lisa Myers, and the NBC News Investigative Unit.

toring radical Internet websites and their users, focusing in on one group espousing anti-Western views in particular. Two men in particular piqued their interest: Fahim Ahmad, 22, and his friend Zakaria Amara, 21. By late 2005, the RCMP had launched its own investigation. Mubin Shaikh, a well-known member of Toronto's Muslim community, has gone public with his role as a police agent who infiltrated the alleged cell. Shaikh, who is expected to be a key witness for the prosecution, has admitted that in December 2005 he helped lead what police allege was a "training camp," where men reportedly played paintball games, trained for an attack and made a jihadist video imitating warfare. A second police agent, whose identity has never been made public, reportedly acted as the supplier. On June 2, the RCMP's anti-terrorism task force deployed officers on two fronts: a major undercover operation to deliver three tons of ammonium nitrate and a massive police raid that netted the 17 arrests.

This investigation represents a textbook example of how to conduct intelligence-led policing, or letting the case lead investigators to unravel and take-down the entire network by relying more on community based knowledge, including informants, by patiently running all leads to ground and trying to bring down the entire network, not simply the foot-soldiers or the dons. It shows how interagency collaboration and coordination can yield incredible results and is a case-study for law enforcement to transcend the 'one agent-one case' approach.

Handling Too Much Information

Counterterrorism investigators are often required to analyze vast amounts of data within short time frames. Intuitively, the more information one has at one's disposal, the better outcome one might imagine would result: knowledge is power after all. At the same time, however, the reality is that most law enforcement agencies are understaffed, under-funded, lack the necessary tools for conducting automated data exploitation and the deep substantive expertise in-house to allow them the ability to quickly scan, filter and use that information to benefit that investigation. There are, therefore, two challenges for investigators: acquiring as much relevant information as possible and finding the necessary resources to analyze and use that information in a way that supports ongoing investigations.

On the side of collecting information, the Australian counterterrorism community has handled this challenge by establishing a national security telephone hotline. The hotline has proven a valuable tool for connecting and investing the national public into their attempt to identify and pursue leads related to terrorist threats. The hotline receives about 1000 calls a month and every call does require some level of follow-up by investigators, which invariably consumes resources and manpower. The Australian government has decided, however, that the benefits wrought by such an initiative outweigh the bureaucratic costs. Government officials do acknowledge though, that only some of those calls have led to active investigations.

Other communities have sought to establish similarly minded programs like New York City's "If you see something, say something," program. Building on the success of its widely recognized "See Something, Say Something" security awareness advertising campaign, the MTA has unveiled a new series of posters that reinforce the effort to enlist customers to join the police and MTA employees as the eyes and ears of the system. The new in-system posters present photographs that show bags left in various transit locations on subways, trains, buses, and platforms and add a new element: Be Suspicious of Anything Unattended. Their goal is to raise customer awareness of the types of potential threats and to report such items to an MTA employee, a police officer, or the anti-terrorism hotline, 888-NYC-SAFE. The posters draw on the lessons transportation officials have

learned in the past two years, especially from meetings with transportation officials from Madrid after the March 11 railroad bombings, said MTA Executive Director Katherine N. Lapp. According to William A. Morange, the MTA's director of security, officials in Madrid said that several passengers interviewed after the bombings remembered seeing the unattended knapsacks that turned out to contain the bombs, but did not alert anyone. The posters feature a bright yellow-orange background.

The MTA expects that the new campaign will lead to many reports that prove harmless—a result it is willing to live with—and are working to find ways, especially in the subway system, to minimize the schedule delays they cause when police officers and bomb-sniffing dogs are called in to investigate. Since March, the MTA has received many more calls, and its bomb-sniffing K-9 units, which respond to calls of suspicious packages in Metro-North Railroad and Long Island Rail Road stations, Grand Central Terminal, and Penn Station, have been increasingly busy. They responded to 71 calls in January, 104 in March, and 124 in April.

Sometimes, the vast amount of information combined with the need for one agency to deliver information to another agency can lead to mistakes. During the 2007 Glasgow airport attack, Australian investigators sought to aid their British colleagues. "The organisation and the investigation team in particular has worked to a deadline to achieve those ends, and at the same time meeting some of the obligations that we have at an international level to provide some answers back to the UK," he said. Australian investigators also pointed that they had a very basic problem in communicating what relevant information that they did find given the massive time difference between them and the United Kingdom, making it nearly impossible to carry-on extended conversations during normal business hours.

The fact is, however, that when the British government acknowledges publicly that, "up to two dozen" counterterrorism investigations are operating across the country at any given time, the ability to concentrate limited resources and make clear distinctions between the prioritization of investigations, the differences and relationships among domestic terrorism cells, and the tracking of financing streams from source to cell becomes a very complicated business. "Despite the apparent breakthrough, it would be wrong to assume that in the case of groups like Al-Qa'ida it is a question of just one throw of the dice," one source said. "There are a series of interlocking cells. Cells overlap... certainly in this case, we can't be certain that everything has been disrupted."

Public Investigative Mistakes

Because of the highly public nature of counterterrorism investigations that occur in the immediate aftermath of an attack, investigative missteps often become front-page news stories. Consider the incident occurring after the May 11, 2004 al-Qa`ida styled synchronized bombing train bombings in Madrid, Spain in which 191 were killed were wounded as a result. Investigators, desperate for leads, found what they believed to be a fingerprint from a suspect named Brandon Mayfield, an American convert to Islam practicing law in the United States. The FBI assisted Spanish police by comparing latent fingerprints found nearby on a bag of detonators against its massive fingerprint database, which includes prints from former U.S. soldiers. Mayfield served in the U.S. Army.

Two FBI examiners and a unit chief eventually narrowed the fingerprint match to Mayfield. Spanish police conducted their own analysis and concluded that the print was not Mayfield's. The FBI disputed that finding, dispatching an examiner to Madrid to press its case. Mayfield was arrested three weeks later amid media leaks about the ongoing investigation. The case has become a potent symbol for civil liberties advocates who argue that

it shows how easily the government can abuse its powers to detain alleged terrorism suspects under relaxed standards of probable cause.

Justice Department spokeswoman, Tasia Scolinos, issued a statement emphasizing that the FBI was not aware of Mayfield's Muslim faith when he was first identified as a suspect and that investigators "did not misuse any provisions of the USA Patriot Act." Scolinos also said the FBI has implemented reforms to avoid a similar mistake in the future. A report released in March by Justice Department Inspector General, Glenn A. Fine, found that although Mayfield's religion was not a factor in his initial identification, it contributed to the FBI's reluctance to reexamine its conclusions after challenges from Spanish police. Fine also found that the FBI used expanded powers under the Patriot Act to demand personal information about Mayfield from banks and other companies, and that the law "amplified the consequences" of the FBI's mistakes by allowing other government agencies to share flawed information. The U.S. government did agree to pay $2 million in order to settle the lawsuit. Under the terms of the settlement filed in U.S. District Court in Portland, the government also issued an apology to Mayfield for the "suffering" caused by his wrongful arrest and imprisonment. It acknowledged that the ordeal was "deeply upsetting" to Mayfield and his family.[60]

Recently, Australian counterterrorism investigators made a similarly public misstep in accusing Dr. Mohamed Haneef with having provided support to a terrorist organisation plotting attacks in Britain by giving his mobile phone SIM card to a relative later linked to the failed plan to bomb central London and Glasgow airport. The Australiian commonwealth Director of Public Prosecutions (DPP) ended up dropping the terror charge in the Brisbane Magistrates Court against Haneef after a review of the investigation, on the basis that Haneef's arrest was a mistake.

It was revealed during the course of the review that Haneef's SIM card was not found at the scene of the Glasgow attack, as Commonwealth prosecutors had alleged at Haneef's bail hearing, but in Liverpool. "I've never seen such an incompetent explanation of what's going on from the Federal Government," Haneef's defense attorney said to the press.[61] The Australian DPP responded in an attempt to defend the process, saying, "The police investigation has been thorough, I make no apology for that, nor should I in a terrorism investigation in this country." We have done our job well in this instance, we have done our job professionally."

In another Canadian counterterrorism case, the name of a possible "peripheral witness" in an anti-terrorism investigation of two other men was given to U.S. authorities by the Royal Canadian Mounted Police, a key counterterrorism investigative arm of the Canadian government. The U.S. entered the name on its "Visa Viper" flight watch list for possible terrorism suspects, which itself has been plagued with problems, not the least being the mistaken entry of the name of U.S. Senator Edward Kennedy as an individual banned from air travel as a security risk. When this individual tried to fly to the United States and was denied, the case became a public headache to the Canadian government, who had to then determine whether he should have been on the blacklist or not.

In an effort to avoid these mistakes, Transport Canada has been trying to create a domestically produced no-fly list that is as error-free as possible. "We want to get it right the first time," said Vanessa Vermette, a spokeswoman for Transport Canada. Transport Canada has yet to publish final regulations for this list, however, leaving commercial air carriers to sort through the mess of foreign

60 Dan Eggen, *U.S. Settles Suit Filed by Ore. Lawyer, $2 Million Will Be Paid For Wrongful Arrest After Madrid Attack*, Wash. Post, Nov. 30, 2006, at A03.

61 Cosima Marriner & Sarah Smiles, "Haneef 'not a significant focus' of UK inquiry," The Age, July 23, 2007.

databases, partial and problematically constructed watch lists and the best instincts of employees when deciding to deny someone a boarding pass as a security risk. The challenge to the creation of this list is that passengers may be blacklisted as a security risk even if the supporting intelligence does not meet the evidentiary threshold that would allow authorities to issue an arrest warrant. In an effort to deal with this impending problem, Transport Canada officials say they plan to incorporate an appeals process so that passengers blacklisted by mistake can get their names removed from the list.[62]

Special Circumstances

Sometimes agencies involved in counterterrorism investigations encounter new and unforeseen circumstances. The Dutch General Intelligence and Security Service (AIVD) had not been actively monitoring what its translators did with the material on which they were working. Supervisors left it up to the translators themselves to decide which tapped conversations should be kept and which could be discarded on a daily basis. One former AIVD translator, Outman Ben A., has been accused by the AIVED of leaking state secrets to radical Muslims. Ben A., a Nijmegen resident of Moroccan origin, was arrested on 30 September 2004 on suspicion of violating state secrecy and leaking information to individuals suspected of terrorism. Ben A. was involved in a high-profile counterterrorism investigation, likely that of the Hofstad network during which time he allegedly leaked highly confidential information to this network in Amsterdam. On 25 September 2003, the AIVD received information to the effect that a person from an Islamist terrorist network had AIVD information. The next day, police raided the home of Hassan O. in Utrecht, and found two A4 sheets containing secret AIVD information. "Mushabarad," the Arabic term for "secret service," was written on one of the letters found. After Ben A.'s arrest, the AIVD sought to publicly minimize the damage that this translator had caused to the investigation but more information is presumed to have been leaked to the terrorist cell.[63]

In other cases, no centralized investigative effort exists until it is started in the form of a special task force. Consider the aftermath of the Mumbai train bombings that killed 11 and injured more than 70 others. Maharashtra Chief Minister, Sushil Kumar Shinde, came out immediately after the attack arguing that it was unreasonable to expect the intelligence agencies to have averted the blast. Because they were working with very little background knowledge on the cell that perpetrated the attack, the state government had to set up a special terrorism investigation cell from scratch. After facing extensive criticism, the state government sought to publicly respond, both in the form of prevention and investigation: they increased the number of nakabandis [checkpoints] and began investigating specific leads into the case. The state had received intelligence reports, for instance, of possible strikes on August 15, January 26 and December 1.[64]

Future Challenges for Counterterrorism Investigations

Thirteen Moroccans standing trial in Brussels in 2007 posed a major test for the new antiterrorism act and the investigation methods used by the Belgian police and State Security Service. The investigation, according to a recent report, began in 2002 when police in Maaseik, a municipality in the Limburg province of Belgium, received an anonymous phone call from someone about three non-native Limburgers: Abdallah Ouabour, Khalid Bouloudo, and Lahoucine al-Haski. The three, the caller reported, had recently made a trip to the

62 Jeff Sallot & Colin Freeze, *Four Years Later, No-Fly List Remains Grounded; Air Carriers Left With Only a Hodgepodge of Databases, Partial Watch Lists, Instincts,* The Globe and Mail, July 06, 2006.

63 Rotterdam NRC Handelsblad, "Poor Monitoring of AIVD Translators," Jan. 08, 2005.

64 The Asian Age correspondent, *Mumbai bomb was very sophisticated*, New Delhi, The Asian Age, Mar. 15, 2003.

Middle East and they had gone from well-integrated citizens to outwardly devout Muslims with long beards and conservative dress. Such tips had become increasingly common, both in Belgium as well as throughout Europe as citizens became more focused on sudden behavioral changes of Muslims.[65]

The Maaseik police, however, did communicate the tip the Belgian State Security Service, prompting the creation of, "Operation Asparagus," the first mention of which occurred on Christmas Eve in 2002, when the Belgian Security Service bugged the telephones of a snack bar and two cyber cafés, shadowed and photographed suspects and conducted covert searches of their homes. The service also gathered information with foreign secret services and Interpol, the international information service of the police. About six months later, the Moroccan secret service called the Brussels-based office of the State Security Service with the message: "During an interrogation with Nouredine Nafia, a Moroccan citizen and the cofounder and one of the leaders of the GICM who has already been sentenced to 20 years imprisonment, he revealed the names of the members of the Belgian GICM branch."

GICM, or the Moroccan Islamic Combatant Group, is a radical Islamic movement which came into being in the wake of the Afghan Mujahidin resistance movement against Soviet troops. The suspect also told his interrogators that the movement has dormant cells in the United Kingdom, Denmark, Egypt, Turkey, Morocco, Spain, France, and Belgium. Brussels immediately requested all available information on the names given to them, and, according to the report, Belgian investigators went to Paris and Casablanca themselves to begin acquiring more information. Wherever the police put suspected GICM members behind bars, Belgian investigators turned up with photographic records and reports of the Belgian Security Service. In a prison in Paris, six GICM members confirmed Nafia's statements to Belgian investigators, who, although had never heard of the names of the Belgian suspects, did recognize their faces in pictures.

Since March 2004, right after the Madrid attacks, some of the suspects were being kept in pretrial custody in the jails of Vorst and Sint-Gillis. Three other suspects would be arrested in September 2004. The 13 GICM members who are now standing trial in Brussels have been charged of several criminal offenses, including recruiting terrorists, criminal association with a view to perpetrating attacks, raising funds for terrorist attacks, and forging passports and other documents (for some suspects, this is the only charge). For most of the cell, however, the public release of details in their cases reveals only one corroborated link between all 13 of them. The media has pounced on this seeming lack of clear evidence among the suspects.

In other cases, the link between cell members, however, was much more overt and concerning: they exchanged phone numbers and stored them -- some of them in coded format -- in the address books of their mobile phones. On some occasions, two suspects were involved in the same penal offense: Mourad Chabarou, a friend of the two Madrid suspects, was allegedly implicated in an armed robbery; Rachid Iba lent his passport to smuggle Lahoucine al-Haski into Belgium; Khalid Bouloudo was reportedly even photographed in Usama Bin Ladin's company. When the house of Mostafa Lounani was searched, the authorities found some diagrams of metal detectors and a hastily drawn schematic of a detonation device for a mobile-phone-controlled bomb. The question is whether these charges will suffice to put the 13 suspects in jail for 15 to 20 years. One of the defense attorneys publicly argued that "despite all phone taps, observations, and special investigation methods, the 28,000-page dossier does not substantiate a single hard fact." He said, "They

65 Frank Demets, *Fundamentalist or Terrorist?* Brussels Knack, Nov. 16, 2005.

have no confessions, no concrete plans of attacks; they even do not have any recordings of conversations in which the suspects discuss the Madrid or Casablanca attacks. If the legal authorities in Northern Ireland used the same rigid rules as the Belgians do, 50 percent of the Belfast population would be in jail. Since January 2004, however, when the Belgians established their new antiterrorism act, the legal definition of terrorism is no longer limited to plotting or perpetrating attacks. At the trials of Nizar Trabelsi and Tarek Maaroufi, both of whom were convicted by a Belgian judge, the legal authorities still had to prove the existence of such plans. At present, however, one can be brought before a criminal court simply for having maintained contacts with terrorists -- although the Council of State in its evaluation of the bill strongly recommended using the "most restrictive interpretation of terrorism." As news reporting has identified, the GICM trial will therefore be a serious test for the new antiterrorism act and lead to a heated discussion on the means and purpose of the investigation.

Conclusion

The United States government, as do other governments, faces innumerous challenges in its ongoing effort to improve America's ability to conduct counterterrorism investigations. Some of these challenges center around collecting and handling information, including, recognizing and designating "terrorism" information as such; protecting operationally sensitive information while making it as widely available as necessary and ensuring that constitutional rights of individuals are not violated through information sharing practices. Other challenges revolve around the organizational and bureaucratic reality of investigating terrorist plots, including, clarifying roles, responsibilities, and information needs of the members of the counterterrorism community; developing a considered approach to information sharing across Federal, state, and local levels in ever increasing numbers of networks and databases emerge. Finally, there are the basic challenges of investigating highly complex, opaque and fluid organizations underwritten by an ideology that is poorly understood in this country.

Those involved in counterterrorism investigations must therefore be innovative, flexible, aggressive and persistent in doing their jobs. Bureaucratic structures do not typically evolve to meet current threats until the threats have themselves already morphed again. It is therefore imperative that law enforcement, homeland security, first responder and intelligence professionals gain the necessary concepts and insights about this enemy that they need to act dynamically in a dimly lit environment.

Chapter 7

International Approach

Synopsis

7.1 Freedom of Information in the State of Israel Legislation, Assimilation and Case Law

by Nissan Ratzlav-Katz and Ranan Tal

Introduction

This paper sets forth an overview of Freedom of Information (FOI) legislation and related major case law of the State of Israel, as well legislative or judicial exemptions and exceptions to those laws as of May 2007. In addition, the paper will provide a general overview of public and professional perceptions of Israeli FOI legislation, and the level of assimilation of those laws.

Part I of this paper opens with a description of the main provisions of Israel's Freedom of Information Law, 5758-1998, the FOI Law's statutory exceptions, exemptions and limitations, as well as its subsidiary legislation. In addition, Part I presents a brief overview of certain laws that include provisions relevant to FOI.

Furthermore, in order to present Israeli freedom of information legislation and exceptions in a manner most coherent with the "State Open Government Law and Practice in a Post-9/11 World" document supplied by the Center for Terrorism Law at St. Mary's School of Law, Part I includes a thematic subdivision of the FOI exceptions into the categories delineated in the aforementioned document: critical infrastructure; cyber security; first response; political structure; public health; and terror investigations.

Following the legislative overview, Part II of this paper presents major case law surrounding the issue of freedom of information in Israel. Part II will summarize major relevant cases preceding passage of the FOI Law that contributed to its legislation. Part II will also present an overview of security-related case law from the period after passage of the Freedom of Information Law.

Part III addresses public and professional perceptions and assessments of FOI legislation, as well as the level of assimilation of the FOI provisions on the part of state authorities and public bodies.

Part IV notes the changes, if any, in Israeli FOI legislation and practice as a result of the 9/11 attacks in New York and Washington in 2001 and their aftermath.

Part I - Public Information Legislation, Exemptions and Exceptions

The primary legislation governing the right of the public to access information collected and held by public bodies in the State of Israel is the Freedom of Information Law, 5758-1998[1], which declares

1 http://www.police.gov.il/english/Information_Services/Law/xx_5759_1998.asp, last viewed June 29, 2007. Note that the translation of the provisions of the Freedom of Information Law used in this paper is, to a large extent,

in Section 1: "Every Israeli citizen and resident has the right to obtain information from a public authority, according to the stipulations of this law." The law went into effect as of May 1999.

A "public authority" for the purposes of the FOI Law (as per Section 2) is any governing or legislative body, municipal or national, any court or other judicial authority established by legislation, any company owned or operated by the national or municipal government, and "[any] other agency fulfilling a public function, which is a controlled agency... as determined by the Minister of Justice, with the approval of the Knesset Constitution, Law, and Justice Committee; such a ruling may apply either to all the activities of the agency, or only to certain activities." "Information" is defined by Section 2 of the FOI Law as, "Any information in the possession of a public authority, whether written, recorded, filmed, photographed, or computerized."

Section 12 of the FOI Law sets forth the restricted right to public information ascribed to a non-resident, non-citizen of Israel. The law will apply to such an individual only "regarding information concerning his rights in Israel."

The FOI Law mandates the designation of an employee in each public authority who will be responsible for implementation of the provisions of the law (Section 3). The public authorities are also required, under Section 5 of the FOI Law, to publish an annual report on their activities and functions.

A request for information under the FOI Law is to be submitted in writing to the designated employee in the public authority from which the petitioner is seeking information (Section 7(a)). The petitioner's request must be answered within 30 days, although this period can be extended for a maximum of an additional 30 days (Section 7(b)). Section 7(a) of the FOI Law stipulates explicitly that the petitioner "shall not be required to state the reason for his request."

In the event of a request for information about a third party or that is liable to harm the interests of a third party, the public authority must inform said third party of the request (Section 13(a)). The third party then has 21 days to file his objections to release of the information. Third party objections may be "pursuant to the stipulations of any law" (Section 13(a)) and may result in a full or partial rejection of the petitioner's information request.

In the event of a rejected request for information or a rejected third party objection, there is no statutory process to challenge the decision within the public authority, but the petitioner or the affected third party is entitled to appeal the decision to an Administrative Court within 30 days of the rejection (Section 17 (a)). The court has the discretion to order release of all or part of the information requested by the appellant (Section 17(d)).

Exemptions, Exceptions and Limitations

Several partial, conditional or absolute statutory limitations on the right to obtain information from government agencies are delineated in three separate sections of the FOI Law.

Section 8 entitles a public authority to reject a request for information in the event that there exists a technical difficulty of some kind in obtaining the information, or that to do so would require "an unreasonable allocation of resources," or that the information can be obtained through another accessible source.

Section 9 defines "information that must not be provided, or that there is no obligation to pro-

original to ITRR and Nissan Ratzlav-Katz or modified from the foregoing English text on the Israeli police web site. The web reference is provided herein for reader convenience. An online Hebrew version of the FOI Law can be found on the Knesset web site, at http://www.knesset.gov.il/laws/special/heb/freedom_info.htm (last viewed June 29, 2007).

vide." 9(a) lists the types of information that may not be released to the public. This includes information that may harm national or individual security or safety, national foreign relations, or an individual's privacy, as well as any information otherwise statutorily forbidden from publication. In addition, Section 9(a)(2) prohibits the publication of "information on matters regarding which the Minister of Defense, for reasons of preserving state security, has specified in an order, with the approval of the Joint Committee[2]."

As distinct from information that may not be released, Section 9(b) lists categories of information that "a public authority is not obliged to provide...." This includes any information:

1. the revelation of which may "disrupt the proper functioning of the public authority;"

2. regarding public policy still in formation;

3. "regarding negotiations with a concern or person outside the public authority;"

4. regarding internal discussions of the authority, including "recommendations given for purposes of decision-making, except for consultations established by law;"

5. "concerning internal management of the public authority, which does not concern the public, and is not of importance to it;"

6. "to which commercial or professional confidentiality applies.... [or] concerning commercial or professional matters linked with a person's business, the disclosure of which is liable to cause real harm to his professional, commercial, or economic interests, except for information that is (a) information about materials emitted, spilled, removed, or discharged into the environment, or (b) results of noise, odor, or radioactive measurements not conducted on private property;"

7. "obtained by the public authority on condition of confidentiality, or that the disclosure of which is liable to jeopardize the obtaining of further information;"

8. "concerning the work methods and procedures of a public authority engaged in enforcing the law, or which has legal authority to investigate, supervise, or clarify complaints, if disclosure of the information is liable to (a) harm action to enforce, supervise, or clarify complaints made to the authority, or (b) harm investigative or legal processes, or the right of a person to a fair trial, or (c) cause the disclosure, or possibly lead to the disclosure, of the existence or identity of a confidential information source;"

9. "concerning the disciplinary affairs of a public authority employee....;" or

10. "the disclosure of which will affect the privacy of a deceased person."

Most court appeals filed pursuant to the FOI Law have followed such 9(b) rejections of information requests.

Section 10 guides the public authority in issuing a rejection of a request for information: "In considering a refusal to provide information under this law, based on the provisions of Section 8 and 9, the public authority will take into account, among

2 A joint committee of the Knesset Constitution, Law and Justice Committee and the Knesset Foreign Affairs and Defense Committee (the "Joint Committee"). According to Section 15 of the FOI Law, "(a) Meetings of the Joint Committee shall be classified, unless decided otherwise; (b) The Joint Committee is entitled to determine that an order approved by it under Sections 9 or 14 shall not be published in the Official Gazette of the Israeli government, either all or in part."

other things, the interest of the applicant in the information, if cited in the request, and the public interest in the disclosure of the information, for reasons of maintaining public health, security, or the environment." Pursuant to Section 11, a public authority may also disclose partial information, rather than issuing a blanket rejection, identifying the information as such (unless doing so will harm the state or any person under Section 9(a)(1)).

Section 14 lists those state agencies and authorities that are exempt from the FOI Law, and to which, therefore, the provisions of the FOI Law shall not apply. They are (subsection 14(a)(1) through (11)):

1. "intelligence agencies of the Israel Defense Forces, and other military units that the Minister of Defense, with the approval of the Joint Committee, has listed in an order, for reasons of state security;"

2. "the General Security Services (GSS) and security units in public authorities, in matters directed by the GSS or on its behalf;"

3. the Institute for Intelligence and Special Tasks (known colloquially and internationally as "the Mossad");

4. the Ministry of Defense's Security Unit;

5. "units in the Prime Minister's Office and the Ministry of Defense dealing primarily with state security or foreign relations," as determined by specific order;

6. "the Israel Atomic Energy Commission, and the nuclear research centers for which it is responsible;"

7. "the Ministry of Foreign Affairs Center for Political Research, disarmament affairs division, policy planning division, and other Ministry of Foreign Affairs divisions that the Minister of Foreign Affairs, with the approval of the Joint Committee, has listed in an order, for reasons involving state security or foreign relations;"

8. "any agency or authority with legally delegated investigative authority, regarding information collected or accumulated for investigative purposes, and regarding intelligence information;"

9. "the Israel Police intelligence and investigative apparatuses, and additional units that the Minister of Internal Security, with the approval of the Joint Committee, has listed in an order;"

10. "the Israel Prison Service – regarding its intelligence and security apparatuses;" and

11. "any quasi-judicial authority whose function is to discuss the medical situation of a person – regarding its internal processes."

In addition, subsection (d) exempts from the provisions of the FOI Law any information or records that a public authority transferred to the state archives pursuant to the Archives Law, 5715-1955.

Subsection (b) of Section 14 authorizes the Minister of Justice, with the approval of the Knesset Constitution, Law and Justice Committee, to temporarily add an authority, agency or category of information to the foregoing list. The period of such an order shall not exceed six months.

Subsection (c) authorizes the Minister of Justice, with the approval of the Knesset Constitution, Law and Justice Committee, to exempt from the FOI Law any corporation founded by a municipal authority or any corporation established by law, "while taking due notice of the degree of harm liable to be caused to the economic or business activity of the corporation."

Subsidiary Regulations and Orders

Shortly after passage of the Freedom of Information Law, 5758-1998, the ministers authorized thereby to formulate regulations, or to extend or delimit the law's provisions, issued several subsidiary orders and regulatory provisions:

1. Freedom of Information Regulations, 5759-1999, pursuant to Sections 4, 5 and 19 of the FOI Law, determines the time and place for the required publication of a list of all public authorities, their respective administrative regulations and bylaws, their annual freedom of information reports, the annual reports of the public authority personnel charged with implementing the provisions of the FOI Law, as well as the bylaws of municipal authorities.

2. Freedom of Information Regulations (Fees), 5759-1999, determines the fees to be charged in connection with every request for information submitted to a public authority, and the limitations and exemptions thereof. Three fees are fixed in these regulations: a fee levied upon making a request for information; a handling fee for locating and sorting the requested information, set according to a fixed hourly rate; and a production fee, levied to cover costs of making a copy of the requested information. Delivery or processing of the requested information is dependent on payment of the foregoing fees.

   An individual requesting information about himself is exempt from the request fee and partially exempt from the handling fees. A public authority may not charge a request fee or a handling fee for information that it is obligated to publicize pursuant to Section 6 of the FOI Law (administrative regulations and municipal bylaws).

3. Freedom of Information Order (Defense Ministry Units to Which the Law Will Not Apply), 5759-1999, pursuant to Section 14(a)(5) of the FOI Law, extends the exemption of security-related agencies from the requirements of the FOI Law to include the Weapons Development Authority and the Weapons and Technological Infrastructure Development Administration.

4. Freedom of Information Order (Police Department Units to Which the Law Will Not Apply), 5759-1999, pursuant to Section 14(a)(9) of the FOI Law, extends the exemption of police intelligence and investigative units from the requirements of the FOI Law to include the Special Counter-Terrorism Unit, the Negotiations Unit, and the Bomb Technicians Squad.

5. Freedom of Information Order (Prime Minister's Office Units to Which the Law Will Not Apply), 5759-1999, pursuant to Section 14(a)(5) of the FOI Law, extends the exemption of security- or foreign affairs-related agencies from the requirements of the FOI Law to include the Prime Minister's Diplomatic Adviser, the Army Secretariat, the National Security Council, most departments of the Nativ intelligence organization, Prime Minister's Office personnel in charge of informants, and the Biological Research Institute.

6. Freedom of Information Order (Subject Matter About Which a Public Authority Will Not Provide Information), 5759-1999, pursuant to Section 9(a)(2) of the FOI Law, designates certain information that may not be provided to the public "for reasons of preserving state security." However, the order specifies that it does not apply to information that the public authority previously made public.

Censored in this order is any information regarding the Israel Defense Force's deployment, bases, operations, units, training, systems, strategies, plans, equipment, preparedness, reserve forces, or stockpiles, as well as budgetary or quantitative information that can reveal the foregoing. The order also prohibits the revelation of information related to: "plans and means of preparing for an emergency in the defense establishment or in the Prime Minister's Office"; the development and purchase of weapons systems; the personal details of personnel in or with the defense establishment whose identities have been concealed by an authorized defense official; security-related joint activities, relationships or trade with foreign bodies, including the existence and activities of defense delegations abroad, and any material, intelligence, know-how or equipment received or delivered in those contexts, or acquired by clandestine means or from confidential sources; the considerations and data forming the basis of government policy regarding foreign security-related trade; the search for missing individuals or hostages, with the exception of someone who has a personal interest in that information.

Finally, the order prohibits the release of any information related to those bodies exempted from the provisions of the FOI Law (Section 14(a)(1-7)) that has been collected or generated in the course of any oversight, control, review, or inter-office activities.

7. Freedom of Information Order (Designation of a Public Authority for Which the Effective Date of the Law is Postponed), 5759-1999. Three such orders postponed for a year or less the effective date of the FOI Law for three specific government agencies: the nation's municipal authorities, the Wages Unit in the Ministry of Finance, and the Nativ intelligence agency. A separate law, the Freedom of Information Order (Effective Date for the Israel Defense Forces), 5759-1999, postponed the effective date of the FOI Law for the armed services until December 31, 2000.

Related and Pre-FOI Law Legislation

Several existing laws and several sections of laws, most of them passed prior to the Freedom of Information Law, 5758-1998, relate to aspects of public access to information. The primary such laws and regulations follow:

1. The Protection of Privacy Law, 5741-1981, was passed to protect an individual's privacy from undue infringement by another. In addition to protection from invasions of privacy (such as spying, eavesdropping, using a person's image for profit, disclosing a person's private affairs, etc.), this law regulates the registration and maintenance of automated databases, both those held by the government (Section 24) and by the private sector. It requires any person maintaining a database to report the existence, use, creation method and protective measures of that database to a governmental registrar.

   Section 13 of this law establishes the right of any person to examine information about him or her held in a database. Exceptions to this provision are (Section 13(e)): databases maintained by the police, military intelligence, the domestic secret service (General Security Services, also known as "Shabak") and the Institute for Intelligence and Special Tasks (also known as "the Mossad"); databases maintained by the tax authorities for purposes of internal information sharing; and when state security, national foreign relations or

any law require that such information not be disclosed. The subsection also allows for the Minister of Justice, in consultation with the Minister of Justice or the Minister of Foreign Affairs, to exempt from public scrutiny databases that include information that state security or national foreign relations require not be disclosed (hereinafter classified information); on the condition, however, that a person may examine information that is not classified information about himself or herself maintained in the same database.

Appeal of a refusal to allow access to a database is to be made before a Magistrate's Court. The penalty for illegally revealing information held in a database, or for not registering such a database, or for using such information for purposes other than those, for which the database was created, is one year in prison. A member of the intelligence unit of the military, the General Security Services, the "Mossad," and the police is exempt from prosecution for violation of the privacy law, insofar as his action was legally authorized.

2. The Archives Law, 5715-1955, establishes the State Archives, a department in the Prime Minister's Office, and determines the deposit and regulation therein of archival material from state institutions or from private individuals. Archival material for deposit in the State Archives is defined as originating in the pre-State period, from authorities no longer in existence, or material that "is no longer required for use and is not permitted to be destroyed...." The State Archivist is responsible for making the archival material available for research.

3. The Secret Monitoring Law, 5739-1979, establishes rules, regulations and limitations on collecting information from or about an individual by clandestine means, especially by concealed listening devices.

4. The Administrative Regulations Amendment Law (Decisions and Reasonings), 5719-1958, affirms and regulates the obligation of a public authority, including the courts, to provide the reasoning behind its decisions in response to requests or petitions from the public.

5. The Criminal Registration Law, 5741-1981 (see Section 12, which establishes the right of a person to examine information about himself or herself in the criminal register).

6. The Patient's Rights Law, 5756-1996 (see Section 13, which establishes the obligation of a medical professional to inform a patient of medical information that will enable the patient to make an informed decision regarding possible treatment).

7. Obligatory Tender Regulations, 5753-1993 (see Section 17(a), which obligates a public authority to provide the tender documents [RFP] to any person or organization filing a request to receive them).

8. Banking Ordinance, 1941 (see Section 15a, which prohibits the publication or revelation of information or documentation received pursuant to the ordinance; a similar provision appears in the Israeli tax code).

9. The State Health Insurance Law, 5754-1994 (see Section 26(e), which obligates the public health insurance agencies to publicize information about their services).

10. Entry to Israel Law, 5712-1952 (see Section 13a(e), which obligates the authorities

to inform an individual held in custody by immigration or security services of his rights).

11. Treatment of the Mentally Ill Law, 5751-1991 (see Section 35(k), which establishes the right of a mentally ill person to receive information regarding his illness).

12. Crime Victim's Rights Law, 5761-2001 (see Section 4(c), which establishes the right of a victim of crime to receive information regarding criminal procedure, his or her rights, and the possible defenses against crime. Subsidiary legislation regulates the publication of information for public use regarding potential defenses against crime).

13. Special Education Law, 5748-1988 (see Section 7, which obligates the responsible public authority to inform parents of the rights of their special-needs child and the various educational frameworks available).

14. Social Workers Law, 5756-1996 (see Section 7, which establishes the right of a person to receive information from a social worker regarding said person's case).

15. Transportation Regulations, 5721-1961 (see Section 195c, which obligates the licensing authority to provide a person seeking or renewing a driver's license the findings of medical tests said person underwent in the context of licensing, as well as the reasoning behind any licensing results thereof).

16. Museums Regulations, 5745-1984 (see Section 10, which obligates museum authorities to publicize information for visitors and the general public regarding exhibitions and activities in public museums).

17. A special case appears in the Emergency Powers Law (Detentions), 5739-1979, which establishes the authority of the Defense Minister to issue an order that an individual be placed in administrative detention; i.e., without charges, and only for reasons of state or public security (for an initial period of up to 48 hours, with subsequent periodic judicial review every three months). Under the regulations governing administrative detention (Section 6(c)), the judge reviewing the detention order is entitled to review evidence in exclusion of the detainee or detainee's counsel and to order that such evidence remain classified.

Exceptions and Exemptions to FOI Laws, by Category

The following is a thematic subdivision of statutory exceptions to Israeli freedom of information provisions as per the categories delineated in the "State Open Government Law and Practice in a Post-9/11 World" document supplied by the Center for Terrorism Law at St. Mary's University School of Law.

Critical Infrastructure

While there are no public information statutes that address this category as *sui generis*, Section 9(a) of the Freedom of Information Law, 5758-1998, prohibits the providing of information that "may harm... public safety..." if made public.

As most infrastructure and utilities companies in Israel are controlled, if not established and operated entirely, by the government, the provisions of the FOI Law apply to them by way of Section 2, which includes such government companies in the definition of "public authority."

Freedom of Information Law, 5758-1998
Section 14(a)(7) exempts "the Israel Atomic Ener-

gy Commission, and the nuclear research centers for which it is responsible."

Freedom of Information Order (Defense Ministry Units to Which the Law Will Not Apply), 5759-1999 The order extends the exemption of security-related agencies from the requirements of the FOI Law to include the Weapons Development Authority and the Weapons and Technological Infrastructure Development Administration.

Cyber Security

Protection of Privacy Law, 5741-1981
Section 2 defines a "violation of privacy" as, among other things, "audio monitoring forbidden by law" (subsection 2), "visually recording a person in his private domain" (subsection 3), "the use of a person's name, title, picture or voice for profit" (subsection 6), "violation of a confidentiality obligation established in law" (subsection 7) or by agreement (subsection 8).

Chapter 2 of the Protection of Privacy Law, "Protection of Privacy in Databases," regulates the registration and maintenance of databases (defined in subsection 7 as a "center for storing information by means of an automatic data analysis system"), both those held by the government (Section 24) and by the private sector: "A person shall not maintain or store a database that is not listed in the Register, and a person shall not use information contained in a database other than for the purposes for which the database was established or the purpose for which the information is intended" (Section 8).

Subsection 12(a): "The Register will maintain in his office a register of databases open to public examination."

Section 13 of this law establishes the right of any person to examine information about himself or herself held in a database.

Subsection 13(a): "Any person, personally or by written power of attorney or such person's legal guardian, is entitled to examine or information about himself or herself stored in a database."

Subsection 13(b): "A person maintaining a database shall present information, requested pursuant to subsection (a), in Hebrew, Arabic or English."

Subsection 13(c): "Information regarding a person's health will not be provided except through a doctor; the doctor shall be permitted to keep information from a requesting party for medical reasons alone."

Exempt from the above freedom of information provisions are: databases maintained by a "security service" (subsection 13(e)(1)), as defined in subsection 19(c) - the police, military intelligence, the domestic secret service (General Security Services, also known as "Shabak") and the Institute for Intelligence and Special Tasks (also known as "the Mossad"); databases maintained by the tax authorities for purposes of internal information sharing (subsection 13(e)(2)); and when state security, national foreign relations or any law require that such information not be disclosed (subsection 13(e)(3)). Subsection 13(e)(4) also allows for the Minister of Justice, in consultation with the Minister of Justice or the Minister of Foreign Affairs, to exempt from public scrutiny databases that include information that state security or national foreign relations require not be disclosed (hereafter: "classified information"); on condition, however, that a person may examine information that is not classified information about himself or herself maintained in the same database.

Section 15: Appeal of a refusal to allow access to a database is to be made before a Magistrate's Court.

Section 17: The penalty for illegally disclosing information held in a database, or for not registering such a database, or for using such information for

purposes other than that for which the database was created, is one year in prison.

Freedom of Information Law, 5758-1998
Subsection 14(a)(8) exempts from the general provisions of the FOI Law "any agency or authority with legally delegated investigative authority, regarding information collected or accumulated for investigative purposes, and regarding intelligence information."

Freedom of Information Order (Subject Matter About Which a Public Authority Will Not Provide Information), 5759-1999
Section 2 exempts from the FOI Law information about, among other things, the Israel Defense Force's training, systems, plans, equipment, preparedness, reserve forces, or stockpiles, as well as budgetary or quantitative information that can reveal the foregoing. Also exempt is information about the development or purchase of weapons systems.

Subsection 2(15) of the order prohibits the release of any information related to those bodies exempted from the provisions of the FOI Law (as per subsection 14(a)(1-7) thereof) that has been collected or generated in the course of any oversight, control, review, or inter-office activities.

First Response

Freedom of Information Order (Subject Matter About Which a Public Authority Will Not Provide Information), 5759-1999
Subsection 2(7): For reasons of national security, a public authority shall not provide information regarding "plans and means of preparing for an emergency in the defense establishment or in the Prime Minister's Office."

More broadly, Section 2 also exempts from the FOI Law information about the Israel Defense Force's training, systems, plans, equipment, preparedness, reserve forces, or stockpiles, as well as budgetary or quantitative information that can reveal the foregoing. Also exempt is information about the development or purchase of weapons systems.

Subsection 2(15) of the order prohibits the release of any information related to those bodies exempted from the provisions of the FOI Law (as per subsection 14(a)(1-7) thereof) that has been collected or generated in the course of any oversight, control, review, or inter-office activities.

Political Structure

The Knesset Foreign Affairs and Defense Committee - one of the two committees that jointly review ministerial requests to add or extend exemptions to the FOI Law - is the only Knesset committee that holds its meetings behind closed doors. It has six subcommittees that also hold classified sessions.

Freedom of Information Law, 5758-1998
Section 14(a)(5) exempts "units in the Prime Minister's Office and the Ministry of Defense dealing primarily with state security or foreign relations, which the Prime Minister or the Minister of Defense has listed in an order, with the approval of the Joint Committee."

Section 14(a)(7) exempts "the Ministry of Foreign Affairs Center for Political Research, disarmament affairs division, policy planning division, and other Ministry of Foreign Affairs units, which the Minister of Foreign Affairs, with the approval of the Joint Committee, has listed in an order, for reasons involving state security or foreign relations."

The "Joint Committee" is defined as consisting of the members of the Knesset Constitution, Law and Justice Committee and the Knesset Foreign Affairs and Defense Committee. According to Section 15 of the FOI Law, "(a) Meetings of the Joint Committee shall be classified, unless decided otherwise; (b) The Joint Committee is entitled

to determine that an order approved by it under Sections 9 or 14 shall not be published in the Official Gazette of the Israeli government, either all or in part."

Public Health

Freedom of Information Law, 5758-1998
Section 14(a)(7) exempts "the Israel Atomic Energy Commission, and the nuclear research centers for which it is responsible."

Freedom of Information Order (Prime Minister's Office Units to Which the Law Will Not Apply), 5759-1999
Subsection 1(6) of the order extends the exemption of security- or foreign affairs-related agencies from the requirements of the FOI Law to include the Biological Research Institute.

Terror Investigations

Freedom of Information Law, 5758-1998
Section 9(a): "A public authority shall not provide...
(1) Information, the disclosure of which may harm state security, its foreign relations, public safety, or the safety or well-being of a person."

....

Section 9(b): "A public authority is not obliged to provide...
(7) Information obtained by the public authority on condition of confidentiality, or that the disclosure of which is liable to jeopardize the obtaining of further information;
(8) Information concerning the work methods and procedures of a public authority engaged in enforcing the law, or which has legal authority to investigate, supervise, or clarify complaints, if disclosure of the information is liable to (a) harm action to enforce, supervise, or clarify complaints made to the authority, or (b) harm investigative or legal processes, or the right of a person to a fair trial, or (c) cause the disclosure, or possibly lead to the disclosure, of the existence or identity of a confidential information source..."

Section 14(a) lists those public authorities given blanket exemption from the requirements of the FOI Law. The authorities relevant for this thematic category alone, i.e., those involved in counter-terrorism investigations and intelligence, include:

1) "The intelligence agencies of the Israel Defense Forces, and other military units, which the Minister of Defense, with the approval of the Joint Committee, have listed in an order, for reasons of state security;"
2) "The General Security Services and security units in public authorities, in matters directed by the General Security Services, or on its behalf;"
3) "The Institute for Intelligence and Special Tasks;"
4) "The Unit in Charge of Security in the Ministry of Defense;"
5) "Units in the Prime Minister's Office and the Ministry of Defense dealing primarily with state security or foreign relations, which the Prime Minister or the Minister of Defense has listed in an order, with the approval of the Joint Committee;"
6) ....
7) "The Ministry of Foreign Affairs Center for Political Research... and other Ministry of Foreign Affairs units, which the Minister of Foreign Affairs, with the approval of the Joint Committee, has listed in an order, for reasons involving state security or foreign relations;"
8) "Any agency or authority with legally delegated investigative authority, regarding information collected or accumulated for investigative purposes, and regarding intelligence information;"
9) "The Israel Police intelligence and investigative apparatuses, and additional units

which the Minister of Internal Security, with the approval of the Joint Committee, has listed in an order;"

10) "The Israel Prison Service – regarding its intelligence and security apparatuses."

11) ....

Freedom of Information Order (Police Department Units to Which the Law Will Not Apply), 5759-1999

The order extends the exemption of police intelligence and investigative units from the requirements of the FOI Law to include the Special Counter-Terrorism Unit, the Negotiations Unit, and the Bomb Technicians Squad.

Freedom of Information Order (Prime Minister's Office Units to Which the Law Will Not Apply), 5759-1999

The order extends the exemption of security- or foreign affairs-related agencies from the requirements of the FOI Law to include, among others, most departments of the Nativ intelligence organization and the Prime Minister's Office personnel in charge of informants.

Part II - Freedom of Information Case Law

Selected Case Law Prior to the Freedom of Information Law, 5758-1998

In the 1962 case, *The Israel Film Studios v. Gary* (HCJ 243/62 16 IsrSC 2407), Justice Landau wrote, regarding the principle of freedom of speech (upheld in the landmark *Kol Ha'am* case, SCD 73/58 *Kol Ha'am Ltd. v. the Interior Minister,* 7 IsrSC 871): "A regime that arrogates to itself the right to determine what is good for the citizen to know, ultimately determines what is good for the citizen to think; and there is no greater contradiction than this to true democracy, which is not directed from above."

In HCJ 337/66 *Pitel v. the Tax Authority of the Municipality of Holon* 21(1) IsrSC 69, the court addressed and upheld the citizen's "right to review information [held by a public authority] in which he has legitimate interest." The court inferred this right to access information "not only from the articles of the law, but also because common sense and elementary decency between the citizen and the government dictates it."

The right of the citizen to information held by the state was again recognized, and further explained, in a 1970 case decided by the High Court of Justice (HCJ 142/70 *Shapira v. Jerusalem District Committee of the Israel Bar Associaton* 25(1) IsrSC 325), in which Justice Cohen wrote:

> The argument that in the absence of any legal obligation to disclose I am entitled to conceal and not reveal, can be proffered by a private individual or body...but it is not available to an authority that fulfills a statutory function....[A] public authority is created solely to serve the community and has no interests of its own. Everything it has, it holds as a trustee and has no additional, different or separate rights or duties of its own, over and above those that derive from its position as trustee or are vested in or imposed on it by virtue of enacted provisions.

In *Zichroni* (HCJ 243/82 *Zichroni v. the Managing Committee of the Israel Broadcasting Authority [IBA]* 37(1) IsrSC 757), the issue was an IBA directive that forbade broadcasting interviews with "public figures" who were known to support the Palestine Liberation Organization. The petitioner argued, and the court recognized, that the public had a right to receive full information about events in Israel and abroad. However, Justice Levin also noted that the said right would not be upheld in the event that, in doing so, "damage would be caused to the vital interests of the State or an individual."

In a later decision (HCJ 680/88 *Shnitzer v. the Chief Military Censor* 42(4) IsrSC 617), which

was important for setting conceptual limits on the security exception to the right of free speech (and by extension, to the right to receive information), the court stated: "Security is a means to an end. The goal is the democratic regime, which is a regime of the people that facilitates personal freedoms." Therefore, the court said, a determination of "near certainty" of real danger was required before censorship of free speech would be allowed.

While the courts had thus far clearly recognized the right of an individual to receive information about himself or herself held by a public authority, and they had likewise defined and clarified the right of free speech, the courts had not yet recognized a right to receive information of public (rather than individual) interest.

In fact, in the 1989 case *Ben v. the Minister of Justice* (HCJ 414/89 43(4) IsrSC 327), the High Court of Justice rejected a petition requesting that the Ministry of Justice provide information on the extent and method of wiretaps carried out pursuant to the Secret Monitoring Law, 5739-1979. The petitioners, as journalists, claimed that their right to the requested information was the natural corollary of their own obligation to provide full and accurate information to the public. The court, however, found that the petitioners were simply unable to demonstrate that the respondents were under any statutory obligation to provide the requested information.

In great contrast, just one year later, in the landmark *Shalit* case (HCJ 1601/90 *Shalit v. MK Shimon Peres and Others* 44(3) IsrSC 353), the High Court of Justice upheld a petition to force the Labor party to disclose political agreements it had reached with other parties in its efforts to form a coalition government. In *Shalit*, the justices emphasized that the matter of publication of information such as political agreements should be regulated by legislation; however, they also agreed that, in the absence of such legislation, they were, per Justice Barak, obligated "to give expression to the basic principles contained in our system of law."

As it was expressed by Justice Shamgar in that unanimous decision, "Freedom of public opinion and knowledge of what is happening in the channels of government are an integral part of a democratic regime, which is structured on the constant sharing of information about what is happening in public life with the public itself. Withholding of information is justifiable only in exceptional cases where security of the State or foreign relations may be impaired or when there is a risk of harming some vital public interest."

Justice Barak said, "From the [public official's] duty of trust follows the obligation of disclosure, as well. ...Information in his possession is not his private 'property.' It is 'property' that belongs to the public, and he must bring it to the notice of the public."

The *Shalit* decision gave a judicial impetus to those seeking to influence the legislature to pass a freedom of information statute. However, there were several failed efforts in the next few years for the Knesset to codify the freedom of information (although a specific obligation to publicize political coalition agreements was legislated). Finally, public pressure and the 1994 establishment of a state committee for the drafting of a proposed Freedom of Information Law eventually led to the ratification of the Freedom of Information Law, 5758-1998.

Selected Case Law Subsequent to the Freedom of Information Law, 5758-1998 - Security and Counter-Terrorism

Since the passage of the FOI Law, as noted by Yuval Rabin and Roy Peled, "Many of the applications submitted to the authorities concern citizens' personal affairs, or other non-controversial matters. Information in respect thereof was provided quite freely even before the Law was legislated." (Rabin, Y. and Peled, R. (2005) "Between FOI Law and FOI Culture: The Israeli Experience" in

Open Government: a journal on Freedom of Information Volume 1 Issue 2; published on July 26, 2005).

Court cases involving rejected petitions for information of interest to the general public have been filed primarily by the Association for Civil Rights in Israel, environmental groups, the Freedom of Information Movement, and journalists. Such cases have been, with time, defining the application of the FOI Law in practice (especially regarding definitional issues, such as the meaning of "public authority" in relation to universities, the meaning of the "internal discussions" exception, as well as the rights of third parties to prevent disclosure, and the like). Most such cases are settled in District Court, in its capacity as Administrative Court, serving as the court of first instance for review of rejected requests for information pursuant to the FOI Law.

The following are three recent cases that focus on or reference security or counter-terrorism issues from the perspective of the FOI Law.

In *The Israeli News Company Ltd. v. the Transportation Ministry* (AA 454/02 2004(2) Takdin-District Court 3587), the court discussed the question of a journalist's right to examine the internal ombudsman's report of a government ministry. After a detailed review of the purpose of the FOI Law and the laws relevant to internal ombudsman's and State Comptroller's reports, the judge notes that the Police Ministry (now the Internal Security Ministry) published the findings of its internal ombudsman despite the partial exemption from the FOI provisions enjoyed by the police department (per Section 14(a)(9) of the FOI Law).

The judge further writes, "There are special instances in which the legislature explicitly determines that internal reports are not to be publicized unless the authority so decided specifically, according to individual considerations on a case-by-case basis. Thus it is in the case of investigations in the military...."

In *The Freedom of Information Movement in Israel v. Israel Airports Authority* (AA 1555/06 [unpublished]) - which the presiding judge called a "fanciful" petition, adding that "it would have been better had it never been filed" - the Freedom of Information Movement requested that the court compel the Israel Airports Authority to provide it with information regarding the standards guiding airport security personnel in security checks, without specific profiling criteria but including the information as to what ethnic origin, religion and gender said profiling is based on, if any.

The Airports Authority acceded to the request in part, providing protocols of the committee for security checks of the Arab population, although only following petitioning of the appeal. The Airports Authority also explained that its security profiling standards are set by the General Security Services, noting that during the last 4-5 years, about 1,600 complaints had been filed by civilians. In response, the appellant requested to know what actions were taken within the Authority, if any, as a result of the aforementioned complaints.

The District Court dismissed the appeal, holding that the Airport Authority security agency falls under Section 14(a)(2) of the FOI Law, stipulating that said law shall not apply to security agencies in public authorities in matters guided or set by the General Security Services, as is the case regarding airport security checks. Furthermore, the court held, the information requested is protected from disclosure under Section 9(a)(1), by which information the disclosure of which may harm state security, its foreign relations, public safety, or the safety or well-being of a person, shall not be provided. The information is thereby also protected under Section 9(a)(4) prohibiting disclosure of information barred by any law.

The court found the appellants attempt to distinguish between "specific profiling criteria" and profiling criteria related to gender, religious and ethnic origin to be an irrelevant distinction. The

said profiling characteristics, the court said, cannot be seen as discriminatory in the context of public safety.

In conclusion, the court determined that the respondent fully answered the appellant's questions regarding the security checks standards, and did not even apply the full extent of the protection provided to it by the law. The criteria used for profiling will remain undisclosed. However, as for the appellant's inquiries regarding the authority's treatment of complaints, this information must be provided to the appellant.

Following the District Court's ruling, an appeal was filed with the Supreme Court by the Freedom of Information Movement. As of June 2007, the appeal has yet to be adjudicated.

In *MK Zehava Gal'on v. the Governmental Committee for the Examination of Events During the 2006 Lebanon Campaign* (HCJ 258/07 [not yet published]), the High Court of Justice heard the direct petition of MK Gal'on that the said Committee publish the protocols of its hearings immediately. The Committee argued that after submitting its entire report to the government, it would publish those sections of the protocols that would not endanger state security or other protected interests.

The High Court of Justice ruled that the basic presumption is that public access to information contributes to, rather than hinders, the judicial or quasi-judicial process. Adjudication in plain view, the court explained, both deters from bias within the judicial system and contributes to public confidence in that system.

The principal of public access was also determined to be based on the public's right to know and on the duty of disclosure to which the public authority is subject, as enacted in the Freedom of Information Law. According to the court, the presumption is that, where not dictated otherwise by interests of national security, the Committee's proceedings must be made public.

Regarding the more general conflict between FOI and national security, the court ruled that the balance between them must preserve national security, but also, and at the same time, must minimize the infringement on the freedom of information. The correct balance of these values cannot be set in advance, for it is a matter of the probability of harm to national security within the specific circumstances of the given case.

Part III - Perceptions and Assimilation

According to several observers of the Israeli legal system and activists promoting freedom of information in Israel, the country does not have a strong tradition of open access to government agencies and information. There is a "basic suspicion" among government authorities of allowing public access to their data, according to Roy Peled of the Freedom of Information Movement in Israel[3], "which is apparently related to the security situation and to a tradition... f centralized government."

The Freedom of Information Law itself, passed unanimously in the Knesset in 1998, was the result of years of intensive work by a coalition of social pressure groups. As Peled and Yuval Rabin write:[4]

"In 1992, a number of non-governmental organizations established the 'Coalition for Freedom of Information.' The Coalition operated several years with both Opposition and Coalition Knesset members, and led to the submission of draft private laws, which never progressed beyond the

3 Interviewed by ITRR on Apr. 12, 2007, at Mr. Peled's organizational headquarters in Rishon Lezion, Israel.

4 Y. Rabin & R. Peled, *Between FOI Law and FOI Culture: The Israeli Experience,* Open Government: a journal on Freedom of Information, Vol. 1 Issue 2, July 26, 2005.

first reading." The draft stated: "In 1994, public pressure led to the establishment of a public committee, headed by a District Court judge (retired), which consisted of a journalist, a representative of the Association for Civil Rights, and representatives from the relevant government ministries. After a year of intensive work, the committee submitted its proposal for the text of the Freedom of Information Law to the Minister of Justice. This proposal was integrated with that of some Knesset members, but three more years of discussions in the Knesset committees, and significant changes in the committee's proposal, were required before the Law was ratified, in May 1998."

Shortly after the passage of the FOI Law, there were some favorable or neutral news and opinion articles in the general media, yet interest quickly waned.[5] However, in more recent years, as more cases have been filed and, in many instances, brought to the attention of the media by interested parties, there has been more general publication of those cases with potentially dramatic public impact[6] (such as the request to publicize the Lebanon War Commission findings, the request for information showing potential conflicts of interest of leading political figures, the request for information regarding the appointment of senior government company directors, etc.).

The professional literature, on the other hand, addressed the issue of freedom of information before passage of the FOI Law. Since then, the literature has primarily focused on FOI Law implementation.

Just prior to the legislation of the FOI Law, Professor Yitzhak Zamir wrote a book entitled *Administrative Authority* (Jerusalem: Nevo, 1996, in Hebrew), in which he reviewed the case law current at the time of his writing regarding the public's access to information. Zamir wrote, "In our writings, we have tried to show that a more balanced and even-handed approach is necessary" when addressing the conflicting values of secrecy and public access. "The burden of proof that secrecy is legitimate and necessary is on the one seeking secrecy, that is, on the government itself. ....These [proposed] measures neutralize the natural adherence of the authority to secrecy and assure greater protection of the right to know and the right to freedom of speech, which are foundation stones of the democratic regime."

In a later book, a seminal work entitled The Right to Know in Light of the Freedom of Information Law (Tel Aviv: Israel Bar Association, 2000), Professor Ze'ev Segal declares, "The right to freedom of information is included in the right of a person to take part in the operation of a democratic regime while knowing the facts." Segal addresses the issue of security and the freedom of information, as well, and concludes that "the appropriate interpretation of the Freedom of Information Law and its exceptions... must give full meaning and legal weight to the *Shnitzer* decision. It is a case that is worthy of being a touchstone for judicial decisions... in appeals of refusal by a public authority to disclose information based on 'concern for harm to state security.'"

Segal claims that the decision in the matter of *Shnitzer* pushed Israeli society "a generation ahead" in relation to the right of the public to receive information in matters of a security-related nature. "The decision has not lost its interpretive inspiration even after ratification of the FOI Law," he concludes.

Former Supreme Court Chief Justice Aharon Barak delivered a speech entitled "Freedom of Information and the Court" in honor of the publication of Prof. Segal's book, in which Barak detailed his own view of the relatively newly minted statutory freedom. His speech was included in the academic quarterly *Kiryat HaMishpat 3* (2003).

5 *Ibid.*

6 Movement for Freedom of Information, http://www.foim.org.il/main/NewspapersArticles.aspx, last viewed June 24, 2007.

In a paper delivered at the 66th Annual International Federation of Library Associations and Institutions in Jerusalem in August 2000, Dr. Debbie Rabina, at the time of Rutgers University, delivered a paper entitled *Access to Government Information in Israel: Stages in Continuing Development of a National Information Policy*. In her paper, Dr. Rabina reviewed the freedom of information situation current at the time and argued in favor of leveraging Israel's library system to facilitate and promote open government provisions and publications.

An important article that has become a basis for subsequent discussions of the FOI Law appeared in the academic law journal *Hamishpat* in 2003. Entitled *The Freedom of Information Law: The Law and the Reality*, by Hillel Sommer, it examined the faulty application of the FOI Law in practice. Suggesting, as have others, that the Israeli public is unaware of its rights of access to information due to the lack of a tradition of open government, Sommer writes, "The Israeli public does not know, at this stage of application of the Freedom of Information Law, how to ask."

Sommer goes on to explain the ways in which the authorities had failed, as of 2002, to implement the FOI Law effectively, if at all. He notes that, often, the individual appointed as the party responsible for responding to FOI Law requests for information was oftentimes also assigned as a spokesperson for the same public authority. Thus, he or she was faced with a conflict of interest in the event that the requested information was not flattering to the organization in question. A second way in which authorities had failed the public was in encouraging the citizenry not to seek information. They did so by means of producing complicated, poor or non-existent FOI materials. As of 2002, Sommer also noted a systematic ignoring of requests filed by the public. Finally, he also claimed that those authorities that did reply to requests often provided capricious and irrelevant refusals to provide information.

Notably, Roy Peled of the Freedom of Information Movement said[7] that the situation has improved somewhat since Sommer wrote his article; however, the public authorities still are relatively reluctant to provide information, so their refusals have become more sophisticated and based around as-yet ambiguous provisions of the law. On the other hand, a brief review of the government web sites shows that they nearly all have Freedom of Information access points (the extent of the information on each site is still limited) and there is a general government web portal[8] that has as its home page an interactive Freedom of Information site declaring, "You have the right to receive information from the public authorities...." with links to various government offices and other types of public information.

In 2005, Dr. Yuval Karniel, one of the originators of the FOI Law, wrote a *Case Comment: The New Freedom of Information Law in Israel is Tested by Its Supreme Court* for Open Government: a journal on Freedom of Information, Vol. 1 Issue 2 (July 26, 2005). In that article, he examined the court's decision in Administrative Petition Appeal 1825/02 *The State of Israel and the Ministry of Health v. the Association of Homes for the Elderly* (unpublished), and argued that the Supreme Court erred in adopting a "balancing test," and rejecting a "special harm test" proposed by a lower court, to determine if the disclosure of a particular piece of information has been justifiably refused pursuant to FOI Law subsection 9(b).

In the same issue of Open Government, Rabin and Peled's article, *Between FOI Law and FOI Culture: The Israeli Experience,* appeared, as well. In it, they, like Sommer, argued that there had been "a very partial implementation of the law." Among other conclusions, Peled and Rabin

7 Interview with Mr. Peled, at Freedom of Information Movement headquarters in Rishon Lezion, Isr (Apr. 12, 2007).

8 Israeli Government, Free Information Portal, http://free.info.gov.il/Lapam/MainPage/main_table.asp, last viewed June 24, 2007.

recommend that there be increasing pressure put on public authorities to execute their obligations pursuant to the FOI legislation by means of administrative supervisory bodies and/or court judgments.

Finally, as a sign, perhaps, of the progress made in FOI awareness in recent years, on Thursday, June 21, 2007, the Almagor terror victims association referred to the FOI Law in a letter its leadership wrote to Defense Minister Ehud Barak. In the letter, Almagor demanded to receive the names of those Fatah terrorists transferred by Israel from Gaza to Egypt and to Judea and Samaria (the "West Bank") in the wake of the Hamas takeover of the Gaza Strip. Almagor also sought the identity of the official who made the decision to allow the transfer and information on how the decision was reached.

"According to the Almagor activists, they have a right to all the information requested under the spirit and provisions of the Freedom of Information Law.... In addition, Almagor referred to the Crime Victims Law, under which "we have a right to know where those who harmed us are located."[9]

Part IV - 9/11

The infamous 9/11 terrorist attacks on New York and Washington in 2001 clearly woke American legislators and political leaders, as well as the American people, to a reality in which their democratic norms of behavior and legislation were suddenly faced with a grave challenge from a clearly undemocratic and cynical domestic and international threat. The subsequent offensive America launched on the centers of terrorism in the wake of 9/11 also presented a challenge of balancing freedom with the need for secrecy.

Israel has been facing the legal and moral challenges of the war on terrorism essentially since its foundation. Therefore, the events of 9/11 and their aftermath did not have any effect on Israeli freedom of information legislation or on security-related case law, other than in passing reference where relevant to the facts of a specific case.

On the contrary, the events of 9/11 and similar events around the world have brought in their wake delegations of officials, law enforcement professionals, attorneys, etc. from around the world - but especially from the United States - to Israel to learn from Israel's bitter and challenging experience in fighting terrorism.[10]

7.2 The French Approach to Open Government in Light of Security Threats Post September 11, 2001

by Vanessa Brochot

"A victim of international terrorism, on its own soil, as well as abroad, France demonstrated long ago its determination to fight all aspects of terrorism, regardless of the perpretrators."[11] Contrary to other countries such as Ireland, the French constitution of 1958 did not include any exceptional juridictional statutes because the political climate at the time did not mandated such foresight, as terrorism did not begin to appear on French soil until much later than the framing of the constitution of the "Fifth Republic." Although French homeland was spared from attacks for a long time, the events of 1970 were to rapidly change the "tone." The legendary passivity of French politics, combined with a heavy "Human Rights" syndrome, inherited from the French Revolution, had contributed to make our country "a welcoming land," if you

9 Israel National News, http://www.israelnationalnews.com/News/News.aspx/122837, last viewed June 25, 2007

10 Israel121c, http://www.israel121c.org, last viewed June 29, 2007. Other examples are linked by Israel21c on this web page, as well.

11 On the ministry of foreign affairs' website "*France and the fight against terrorism*," *available at* http://diplomatie.gouv.fr/fr/france_829/decouvrir_france_4177/france-a-z_225 9/politique-etrangere_2628/france-lutte-contre-terrorisme_6074.html.

will, that some like to rightfully compare-in my opinion-to a haven, much appreciated by foreign terrorists. This, in turn, also had a debilitating effect on terrorism repression in other European countries such as Italy, Germany or Spain.[12]

While the number of total victims is without comparison to that of the events of September 11, I invite you nonetheless, to consult the list of all acts of terrorism commited in France from 1974 until today on the website of "SOS Attentats."[13] French anti-terrorist legislation cannot be studied or understood without taking a close look at the terrorist events which took place on French soil: it is always following such attacks that French anti-terrorism legislation has been enacted as if the law reacted to attacks being perpetrated, attacks which had not been anticipated by such laws.

Following the attacks of the first French terrorist group, General de Gaulle and the OAS (Organization of the Secret Army)[14] set up special jurisdictions to find out who were the authors of these attacks, he then entrusted their judgement to the State Court of Safety.[15] The establishment of specialized jurisdictions is characterized by its derogatory aspect with regards to civil rights, created out of emergency but founded on a text of law, anticipating clearly their conditions and rules of existence; they often appear to be an arbitrary manifestation of the political public power. The State security court was no exception to this "rule:" its derogatory procedure being a "strong" departure from common civil rights (extension of police custody, up to 10 days in the absence formal charges, the authorisation of searches or confiscations as authorized by article 17, the ability to go beyond the basic rights of the parties as to informing them of their rights and of the charges facing them as proposed by article 21, the possibility of extending custody without formal review by a prosecuting magistrate, etc.) was highly criticized, especially more so as this Court would subject individuals to the same statute as military personel and deprived the accused of the right to a trial by jury. In his book. "*The Permanent Coup d'Etat*" published in 1964, François Mitterrand blamed this legislation, thus as soon as he became president in 1981, he removed it following a bill by Robert Badinter, then Minister of Justice. The congressional shuttle rescinded this law (article no. 81-737) on August 4, 1981; the following year another law established that the "crimes and offenses against the fundamental interests of the nation" must be judged under the statute of civil rights legislation.

In light of these elements, it is therefore possible for us to ponder French reaction in regards to the military decree relative to the "detention, treatment and judgement of non-American citizens in the fight against terrorism" which was signed by the President of the United States on November 13, 2001. This decree proposed in particular the creation of exceptional military tribunals to consider judging non-U.S citizens. However, in order to understand "the general indignation" of the international community and of international organizations such as Amnesty International, we must pay closer scrutiny to the aforementioned decree as it includes substantial differences from the French State Security Court document and especially in regards to the contempt of the international standards prohibiting discriminatory treatment based in particular on nationality (as foreign nationals are the ONLY ONES elligible to be tried before these special courts).

12 Fabienne VIRICEL, *Franco-Irish comparative studies of special juridictions in terrorism matters*, study is available on the Juripole website, www.juripole.fr.

13 *See* http://www.sos-attentats.org/justice-liste-attentats.asap?cat_id=Attentats&lan_id=fr

14 The OAS (secret army organization) was a clandestine French political/military organization whose methods were based on terrorist actions. It was created February 11, 1961 after a meeting in Madrid between Jean-Jacques Susini and Pierre Lagaillarde. It regroups the partisans supportive of the "French Algeria" movement through armed conflict. The acronym OAS first appeared on walls in Algiers on March 16, 1961, accompanied by the slogan, "Algeria is French and it will remain French." The name OAS purposely references the Resistance's secret army.

15 In France, the 63-22 and 63-23 laws created the Court of State Security on January 15, 1963.

During the Seventies, another government project created great turmoil: "project SAFARI". This project proposed to identify each citizen by a number and to inter-connect that number to an identification database of all personal administration files. This project raised concerns about the dangers of certain applications for data processing and created worries about general cataloging of the population. It led the government to establish a commission under the auspices of the Ministery of Justice so that the Ministry could put forth specific measures to guarantee that the development of future data processing will include the respect of privacy, as well as that of personal and public liberties. This "Data-Processing and Freedoms Commission," chaired by Bernard Chenot, proposed, after many meetings and much debate, to create an independent authority: the CNIL (National Commission on Data Processing and Liberties).[16] At the end of the year 1977, a bill was reviewed by Congress, before becoming the current law no. 78-17 of January 6, 1978, which relates to data processing in regards to "personal files and freedoms."[17]

The measures undertaken by the socialist government of the time repealed the State Security court, repealed the "Peyrefitte law,"[18] as well as began a policy of decentralization. These measures con-

16 A pluralist electorate composed of 17 commissioners : 4 parliamentarians (2 representatives, 2 senators), 2 members of the economic and social council, 6 representatives of the higher jurisdiction, (2 State advisors, 2 advisors from the Supreme Court of Appeals, 2 advisors from the State Audit's office), 5 qualified personalities appointed by the National assembly's President (1 personality) by Senate president (1 personality), 3 personalities from the council of Ministers. The member's terms of office is of 5 years or for the parliamentarians, of an equal period corresponding to their elected terms. To conduct their missions, the CNIL members rely on various services.
*An independent expert: 12 of the 17 members are elected by assemblies or by their local districts. The CNIL elects its President from amongst its members; it answers to no authority; the ministers, public experts, heads of companies, public or private, cannot oppose the actins of the CNIL for any reason and they must pursue all useful measures to facilitate its task. The president freely recruits its collaborators.
*An administrative expert: The CNIL's budget is applied against the budget of the State. The agents of the CNIL are contracted by the State. The CNIL's decisions can be the object of appeal within the administrative jurisdiction. Facing the dangers to civil liberties that computers pose, the main purpose of the CNIL is to protect privacy and the freedom of the individual. It is given the responsibility of making sure that "Data processing and Liberties" laws are respected, and is therefore entrusted 5 main missions: to inform, to guaranty rights to access, to list public files, to control and to regulate.

17 It would be interesting to conduct a comparative study between the SAFARI project and its American counterpart regarding their aviation/transportation/security dynamics; and the conditions for entry into U.S. territory, which were adopted on November 19, 2001 (the Aviation and Transportation Security Act) and re-enforced on May 5, 2002 by a law which reinforced the conditions for entry into the homeland (Enhanced Border Security and Visa Entry Reform Act). Since March 5, 2003, these measures have imposed standards of communication from the airline companies to customs services and to U.S. security agencies, as well as personnel information relative to their passengers coming from the U.S., under penalty of tighter controls, of fines, and of refusal of landing rights and authorization. Negotiations between the United States and Europe have ended several years of uncertainty regarding the conditions under which the American authorities obtain European air passengers' data and information ("PNR data"). The agreement, which has been ratified, between the United States and the EU, goes back to numerous guaranties that were defended by the European CNIL. The PNR data ("Passenger Name Records") is information which is collected from the airline passengers at the time commercial reservations are made. It allows one to identify the traveler's itinerary, the flights being taken, home contact information (home phone number), custom services requested on flight such as specific dietary preferences (vegetarian, Asian, Kosher, etc) as well as speciall needs requested based on the passenger's health.

18 These two points appeared amongst the 110 propositions of the presidential program of candidate Mitterrand. Peyrefitte's law number 81-82, stated "security and liberties law," extends the matters of police's prerogatives in regards to identity control and red-handed crime, as well as those of the prosecution limiting the freedoms of assessment from a judge, (restricted possibilities for suspended sentences, substitution of sentences and mitigated circumstances) and by so lessening the rights of the defense. This law passed on 2nd of February and it appeared at the JO on 3 February 1981, partially compiled from a decision of the constitutional council - decision number 80-127 DC which was ratified on 19 and 20 of January 1981.

tributed to the temporarily silence the separationist terrorists such as the FLNC (National Liberation Front of Corsica), ETA (Basque Indepence Group), or FRS (Front for the Release of Brittany), although this lull proved of short duration. As early as 1985, a new wave of attacks would engulf France. In reaction, the French Government put in place a special antiterrorist legislation of which the law of September 9, 1986 is the keystone. A new substitute civil rights legislation was then voted into law in order to close the gap in the statute born out of the establishment of the law of 1963 relating to the State Security Court, and in order to allow a quick and effective repression of terrorism.

The question here is not to deny the effects of September 11 on French policy and legislation but to show that the effects of this one event were not as described by the press: circulation of the standards, Patriot Act French style, etc.

The projections with most effect were carried out by the European Union: as of September 12, 2001, the Presidency tasked the following boards "Justice and Interior Affairs," "Transportation," and "Ecofin" (Ecomics and Finance) and challenged them to prepare suitable measures in regards to police response, homeland security, justice and to fight against the financing of terrorism. The Foreign Ministers met the same day, asking the Presidency, the Commission and Mr. Javier Solana to propose an improvement of the joint policy in these fields.[19]

The Ministers of Justice of "the Fifteen" (nation members of the European Union) have, as of 6 December 2001, proposed a framework document relating to the fight against terrorism; a document which makes it possible to blend both the penal legislations of the Member States with regards to the definition and to the sanctions stemming from acts of terrorism. It is not worthy to mention that this legislative framework is largely inspired by the French legislation.

In addition, without the particular context of the attacks of September 11, the European warrant for arrest could not have been set up so quickly, taking into account the reservations expressed by the Italian government. This document blesses the removal of the political control which was traditionally attached to procedures of extradition. "What was a political act now becomes a legal document....We are talking about a major stage in the establishment of a European legal entity. The newly created European warrant for arrest constitutes in itself a genuine mandate for arresting and for turning-over a person. It allows for the direct handing-over of wanted individuals from one legal authority to another, while guaranteeing their fundamental rights and freedoms. This ambitious and innovating project modifies drastically the nature of the penal/legal co-operation: it is no longer a traditional cooperation of State to State but the direct execution of a court order in the spirit of the concept of the recognition of judicial court decisions.[20]

As for France, a country already sensitized to the risks of Islamist terrorism, a European country more affected by international terrorism (not less than 23 acts of terrorism between 1986 and 1996), the effects of September 11 are more about strategic and military reflexion than about the need to reinforce the legal arsenal. An information paper issued by the French National Assembly-report no. 3460[21] (Note: French National Assembly is the

19 Information report submitted and statement given by the National Assembly Delegation for the European Union regarding the fight against terrorism: *A revealing factor in the progress and indequacies of the European Union,* presented by M.Alain Barreau, Representative (Deputy), report no. 3504, registered by the office of the President of the National Assembly on 20 December 2001, page 7.

20 *Ibid*, page 20.

21 Information report submitted and applied through article 145 of the National Commission of Defense regulation and of the armed forces in conclusion of the deliberations of a mission for information on the consequences of the 9/11 terrorist attacks for France. This report (No. 3460, registered with the National Assembly's presidential office

equivalient of the United States House of Representatives) points in this same direction. The report mentions "a rediscovery of the founding principles of defense, globality, and permanence,"[22] it focuses upon the improvements still needed to be carried out in order to fight against terrorism effectively: civil protection, strategic importance of information sharing, military aspects, etc. The attacks of September 11 raise true questions about dissuasion in general and nuclear dissuasion in particular.

In France, the concept of defense was clarified in the first article from edict no. 59-147 dated January 7, 1959, a pilar as it relates to the general organization of defense. The first indented line stipulates that "the object of defense is to insure that at any time, under all circumstances and against all forms of aggression, the safety and the integrity of the territory, as well as the life of the population." The general framework of this ordinance is thus still suitable in the sense that it covers 3 dimensions: a military aspect to preserve the vital interests of the country; a civil aspect relating to the protection of the populations on the territory; and an economic dimension. Ultimately, if the traditional concept of defense, vis-a-vis an enemy identified in a defined state of judicial war, becomes blurred, it is to the benefit of security acts with vaguer boundaries, but the principles of the ordinance of January 7, 1959 are not called into question because of it. On the contrary, what we are witnessing is "a restoration of global defense which is supported within the framework of the fight against international terrorism; the effectiveness of civil means and military personnel resides first of all in their complementarity."[23]

Since 1986, French antiterrorist legislation has been supplemented by 5 new texts. Among all these laws, only the law of November 15, 2001 was not submitted to the Constitutional Council. "This law followed the trauma caused by the attacks of September 11, and the consensual character of the adopted provisions explain the absence of 'saisine.'"[24]. (See Translator's note) The major evolution which followed the events of September 11 in regards to antiterrorist legislation is law no. 2006-64 dated January 23, 2006 which relates to the fight against terrorism and bears various clauses relating to safety and border control. This law, further removed from the events of September 11, caused more criticism.

Still, is it possible to discuss a security drift or a circulation of the standards from the land of Uncle Sam to the Old Continent? Or does it not stem more out of a security movement amplified by the violence and the fear caused by the attacks of September?

First of all, it is important to analyze the impact of the spirit of the enlightenment on the French antiterrorist dispositions (I) then it will be appropriate to analyze, in light of the events of September 11, the evolution of this latter (II).

I. The Imperative French Respect of Rules Melting the State of Right and the Fight Against Terrorism

France, unlike a country such as Ireland, is not simply facing a single independent terrorism.

on 12 December 2001) was presented by Representatives Mr.Paul Quiles, Mr. Rene Galy-Dejean and Mr. Bernard Grasset.

22 *Ibid*, page 68.

23 *Ibid*, pp 71-72.

24 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional Council,* Speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.4.

Translator's Note: "Saisine" - The right of saisine is a unique concept by which a request is submitted to the court for a review of a specific law. The Constitutional Council cannot self-impose such request. When the Council was created in 1958, only four entities were allowed to "seize" such constitutional power: The President, The Prime Minister, The President of the Senate and The Prsident of the National Assembly (House of Representatives). With a revision of the Constitution and by a subsequent Constitutional Amendment dated October 29, 1974, this right has since been extended to 60 representatives or 60 senators, in order to allow a political minority in Congress to ask for control of a specific law in question.

Therefore, it had to obtain a system, both logistical and legal, aimed at suppressing terrorism in all formats (freedom fighters, Radical Communists, Internationalists etc.). As in most countries, French politicians chose to treat terrorism in a global fashion. First of all, it is advisable to study the organisational system (A) and then tie to it this French balance of "safety/freedom" preserved, by the Constitutional Council amongst other entities (B).

A. "Organisational Stakes of the Fight Against Terrorism"[25]

"The policy of combat against terrorism is primarily operational, thus privileging the establishment of means of intervention, without posing the problem of a particular requirement of legitimization."[26] Therefore, the entire challenge of this fight, besides the preservation of human rights, is to insure the cooperation of various branches of government including all the difficulties this implies. France made a conscious choice not to entrust the burden of terrorism repression to a single branch. It is necessary, however, to keep in mind that the difficulties of the fight against terrorism are due more to the fact that the State cannot resort to every means and especially not to means similar to those of the terrorists. The State must fight against terrorism without attacking freedoms, civil rights to which French people and French media remain viscerally attached. Furthermore, both the international and European contexts cannot be isolated and the French government must act in accordance with the agreements ratified and keeping in mind that the building of Europe necessitates bringing together the political attitudes of all member nations.

In order to have a more precise idea of the French antiterrorist fight system, the essential body of work remains the reading of the *White Paper writen by the Government* on the subject of homeland security vis-a-vis terrorism.[27] This combat rests on 4 essential topics:

- to prevent risk, investigate, detect, and neutralize;
- to improve our systems in place;
- to increase our capacities for handling crisis management; and
- to reinforce our capacities for managing sanctions and sentencing.

Taking into account the limited time and the plethora of information regarding these French axes of antiterrorist fighting, I am forced to make a choice in presenting to you only what seems to me primordial, whith the knowlege that this limiting choice will nervertheless deprive us of certain information.

- **Risk prevention:**

Each and every day, this mission mobilizes the services of intelligence, the forces of homeland security, the antiterrorist magistrates, the armed forces and the Diplomatic Corp. More than the co-operation between the various services, it is the access by the services of intelligence and homeland security to certain "public access" administrative files, as well as the identification of the potentially dangerous travelers which must be authorized, and this in spite of the traditional reservations. Until law no. 2006-64 (2006), freedom took precedence over effectiveness and France, contrary to its foreign counterparts, did not have access to the above mentioned files. The co-operation with our foreign partners, initially bilateral, became multilateral because of convergences of interest or because of shared risks with our partners.

- **Improving the system:**

This is about concentrating the protection of the population. It is spearheaded by the "Vigipirate plan" created in October 2001. This plan, well-known by our fellow-citizens, has double objec-

25 Title of a book by Nathalie CETTINA, foreword written by Jacques CHEVALLIER, her memoir's director, Works and research Pantheon-Assas Paris II, LGDJ, Mars 1995.

26 *Ibid*, p.3.

27 French Documentation, March 2006.

tives to protect the population, the infrastructures, and the institutions as well as to plan counterattacks in the event of attacks. The Plan is represented by 4 levels going from yellow, the lowest level, to the scarlet (bright red) level, the highest, and is aimed at preventing the imminent risk of major attacks. Since the installation of the new Vigipirate plan in March 2003, the level of alarms has been adjusted ten different times.

The protection of the population, just like the resolutions resulting from the investigations, cannot be effective without video-surveillance, but France, concerned about the respect of the privacy of its fellow-citizens, lags behind compared to some of its neighbors (to date, there are aproximately 300,000 video cameras on French soil).

- **To reinforce our capacities for crisis management**

- **To reinforce our capacities for repair and sanctions:**

On this matter, France remains a pionneer and the consideration of the victim, beyond the penal lawsuit, is a good representation of the originality of the system of French compensation. "In 1985, the mobilization of the victims gathered within S.O.S. Attacks, constrained the authorities to create by way of legislation, a system of compensation completely disconnected from the penal procedure. Even the term of "terrorism" seemed unacceptable in a context of rights which did not wish to integrate this concept in its own legislation. The legal recognition became accepted only thanks to a mobilization of the public opinion and a public awareness campaign, and by a petition organized by S.O.S. Attacks with the assistance of the media; all the while France was confronted with a new wave of attacks in February and March 1986. In April 1986, a bill relating to the fight against terrorism was submitted to Congress. It called for increased prevention and increased repression against terrorism. The compensation chapter, forgotten initially, was introduced in the form of an amendment. The idea suggested was to de-budgetise the financing of the compensation, so that it would become quick and automatic. Law no. 86.1020 of September 9, 1986 relating to the fight against terrorism and to attacks against the safety of the State mandated by its article 9 a Guarantee fund (hereafter called "the Fund") which guarantees the integral repair of damages resulting from attacks to the individual, as a result of being the victims of acts of terrorism based on article L 126-1 of the Penal code."[28] In accordance with French Human Rights spirit, it is important to stress that the Fund compensates the victims or their dependants, regardless of their nationality or the legality of their residence in France!

The other battle being fought by S.O.S Attacks was to change the status of the victims of terrorism into that of victims of civil war.[29] "This moral recognition allows the victims to benefit from free health care, to access to military hospitals and, for the children affected by terrorism, to access to the statute of war orphan. The victims can also take advantage of the experience of military doctors in regards to post traumatic physical and psychological after-effects. More importantly, beyond this statute, this law recognizes implicitly that terrorism is the new shape of war which touches a civil population during times of peace."[30]

If the French antiterrorist system tries, as much as it can, to maintain this difficult balance between personal liberties and security, even if it means a certain amount of loss in effectiveness, the legal

28 Francoise Rudetzki, *State of the legislation in France: the role played by SOS Attentas*, Terrorism, victims and international penal responsibility, Calman-levy, March 2003, page 232.

29 In article 26 of the law of January 23 (JO 25 January 1990), extending the benefits of the *Code for military pensions for invalids and war victims* to the victims of acts of terrorism committed from January 1, 1982 forward. These have thus been included as victims of war.

30 Francoise Rudetzki, *State of the legislation in France: role played by SOS Attentats*, Terrorism, victims and international penal responsibility, Calman-levy, March 2003, page 236.

arsenal, and more particularly the penal branch, must likewise be registered within a protective framework of public freedoms.

B. The Search for Balance: the Place of the Constitutional Council

Unlike the law of 2001, all the laws adopted in regards to the fight against terrorism are carefully screened by the Constitutional Council which asserts itself as the guardian of fundamental human rights. As recalled by Pierre Mazeaud, President of the Constitutional Council until March 2007, "terrorism indeed represents such a violent attack on law and order and compells such a strong affront upon the authorities, that the risks of compromising the exercise of fundamental freedoms is therefore increased. Therefore, checks and balances to insure constitutionality must be acutely in effect throughout the process."[31] Moreover, if the European Convention on humans right authorizes certain restrictions, under certain conditions, to the basic rights it guarantees, the Constitutional Council reminded us very recently in its Decision no. 2005-532 DC of January 19, 2006 relating to the Law regarding the fight against terrorism and containing various clauses relating to homeland security and border controls, "That it is up to legislators to ensure cooperation between, on one hand, the prevention of attacks on law and order is necessary to the safeguard of rights and principles of constitutional value, and, on the other hand, the exercise of constitutionally guaranteed freedoms and privacy and freedoms specifically protected by articles 2 and 4 of the Declaration of Human Rights and of the citizen of 1789."[32]

Under French law, there is no plan to systematically control legal procedures relating to the fight against terrorism, therefore, such control is optional and *a priori* and this appears to be a fundamental difference between the French and the American systems. "Insofar as antiterrorist legislation constitutes - fertile grounds regarding the potential risks against liberties," Congressional opposition usually seizes control and acts as Counsel in order to exert this control.[33] As previously noted, only the law of November 15, 2001 includes an exception to this rule[34].

This control as applied by the Constitutional Council is divided as follows:
"the Council verifies:

1. that new rules relating to the duration of police custody do not conflict excessively with personal freedom;
2. that any new procedure regarding attorney intervention while in police custody does not conflict needlessly with civil liberties, nor with the rights of the defense, nor with the prerogatives of the legal authorities; and
3. that the clauses regarding vehicle shots and their occupants ensure a balance between the respect of privacy and the safeguarding of law and order."[35]

Let us now take a more concrete look at the impact of the Constitutional Council on antiterrorist laws having been subjected to its review.

The main pillar of French antiterrorist legislation is Law no. 86-1020 dated September 9, 1986 relating to the fight against terrorism improved repression and the prevention of crimes related to terrorism within the penal code. This law, known

31 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional council,* speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.1.

32 9th indented line available on the Constitutional Council website: http://www.conseil-constitutionel.fr/decision/2006/2005532dc.htm.

33 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional council*, speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.4.

34 Law 2001-1062 of November 15, 2001 relative to everyday security.

35 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional council*, speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.4-5.

as the law "Chalandon," set up acts of terrorism as separate infractions punishable with increased penalties. It also established the monetary fund on behalf of victims of terrorism. Furthermore, it specifically, allowed for specialized magistrates specifically appointed to the fight against terrorism, this was made possible by centralizing discovery and trial courts with the Supreme Court of Paris. This was done primarily for reasons of security as well as in light of the unique procedural mode.

In its decision no. 86-213 DC of September 3, 1986, the Constitutional Council decided that only article 4 of the law relating to the fight against terrorism and dealing with attacks against homeland security was declared as not being in accordance with the Constitution; however, the definition of a terrorist act, combined with another crime, or infraction against common law, incriminated by the penal code and by virtue of the connection between these acts "resulting from the actions of one person or several and with the goal to seriously disturb law and order by means of intimidation or terror." The Constitutional Council ruled that the law itself fully satisfied the conditions of precision and claririty required by criminal law. "Crimes of terroristic nature, as well as certain other types of crimes such as those dealing with the traffic of narcotics, are tried in front of courts composed of appointed judges which are all specialized and professional magistrates (a president plus six justices or in case of appeal, eight justices). Notwithstanding common legal procedures, no ordinary citizen is ever called to sit on these panels."[36] Once again, the decision of the constitutional Council ratified this choice which Pierre Mazeaud explains in his text: "In application of its traditional jurisprudence as regards to equality, it was judged that it is permissible for the legislator to take into consideration different rules of procedure according to facts, specific situations, and to the people to which they apply, provided that these differences do not proceed out of unjustified discriminations and that they are ensured justifiable according to guarantees of equality, in particular as it relates to the respect of the rights of the defense.

In regards to this issue, Pierre Mazeaud believes that the differences in established procedures applied to various alleged criminals, according to whether these crimes are terroristic in nature or not, tend to thwart the effect of the threats and could indeed diminish the peaceful rendition of a judgement and that therefore it did not stem from unjustified discrimination. He also raised the point that, by the nature of its composition, the special court offered the necessary guarantees of independence and impartiality and that the rights of the defense were safeguarded when pleading before it."[37]

Furthermore, concerning the lengthening of police custody as proposed by the law of 1986, the law lengthened such custody for a period of up to 48 hours, the Constitutional Council did not object to this decision in consideration of the fact that this lengthening was subjected to medical supervision and related only to acts of terrorism and that it was ordered by a seated magistrate of the special court.

Law no. 90-86 dated January 23, 1990, which contains various clauses relating to social security and public health. This law allows for the victims of acts of terrorism after January 1 1982 to benefit from the same rights and privileges granted to civil war victims in accordance to the Military Code regulating military disability pensions and war victims and, in particular, the right to pensions for civilian victims. In its decision 89-69 DC of January 22, 1990, the Constitutional Council decided in its article number 1 that "in the body of the text of the law carrying various clauses relating to social security and public health; the following are declared to be unconstitutional: - from article 24 to article 27, the words "Of which the Congress will be apprised before December 31, 1990;" and up to article 46, the words "in the overseas territories."[38]

36 *Ibid.*

37 *Ibid.*

38 Constitutional Council, http://www.conseil-consti-

On the occasion of the development of the new penal code, which came into effect on March 1, 1994 and which replaced the imperial (Napoleonic) Penal code dating back to 1810, the legislator has this time around, inserted in the penal code, not as was the case in 1986 in the code of penal procedure, the incrimination of acts of terrorism. "Not only does the New Penal code retain specific terrorism infractions, by reference to acts with which it associates its policy of incrimination, but it furthermore fundamentally innovates by making a clear and basic distinction between three basic types of terrorism: terrorism based on the breaching of commonn law, ecological terrorism, and terrorism by criminal conspiracy."[39] The law which established the new penal code was not presented to the constitutional Council, the latter could not therefore offer an opinon about this extension of the concept of acts of terrorism.

Law no. 95-125 dated February 8, 1995 relating to the organization of the jurisdictions and of the civil, penal and administrative procedures. This text suggests a 30 year term for crimes of terrorism and 20 year term for crimes commited in partnership with a terrorist organization.

Law no. 96-647 dated July 22, 1996 published in the Official Law Review no. 170 of July 23, 1996, following the attacks which took place during the summer of 1995. It is meant to reinforce repression against terrorism and against any attack perpretrated against representatives of the government, against public servants, or against any person whose work involves public interest. The law includes clauses relating to the Department of Criminal Investigation. The Constitutional Council ruled in its article one that: "article 1 is declared to be unconstitutional:"

- because it includes within article 4-421-1 of the penal code the following subparagraph: "assisting with the entry into the country, assisting with the travel or transportation or with the residence of illegal aliens, as defined in article 21 of ordinance no. 45-2658 dated November 2, 1945 relating to the conditions regarding entry and residence of illegal aliens, into France;" and

- words "for the purpose of discovery," "unless they are authorized by the examining magistrate" and the first three subparagraphs inserted by article 10 into article 706-24 of the penal procedural code, insofar as they are aimed toward preliminary investigation cases;

- In regards to article 27 the following words "where it will come into effect on May 1, 1996."

The Constitutional Council "thus did not hesitate in censuring a clause which had been listed among the infringements likely to be described as act of terrorism; offences relating to assisting illegal entry into or assisting with illegal residence in the country.

The Council indeed estimated that the legislator "had sullied its judgement with obvious disproportion," insofar as the measures involved were not material acts of attacks directed toward the safeguarding of property or of people but constituted normal behavior of assistance to people in an irregular situation (in regards to their resident status) and that this was not in immediate relation with the perpetration of an act of terrorism. The Council also noted that if an association with a terrorist group is discovered, the finding of facts could be continued under other sections of the law, such as concealment of criminals or participation in a criminal conspiracy.

"This example attests to a valuable system of checks and balances which gives the Council a

tutionel.fr/decision/1989/89269dc.htm.

39 Yves MAYAUD, Terrorism, Knowledge of the Law, Private Law, Dalloz, May 1997, p.7.

certain margin for independent decision making which is not negligible."[40]

Law no. 2001-1062 dated November 15, 2001 relating to "daily security." Following the attacks which occurred in the United States on September 11, 2001, the French government put into effect certain measures meant to "fight more effectively threats from terrorism." These measures, which were announced by the Prime Minister on October 3, 2001 in front of the French National Assembly, were presented as amendments to the law on daily security, during a Session of the congress. Emergency regulations were therefore adopted, without being submitted to the Constitutional Council.

Constitutional law no. 2003-267 relating to a European warrant for arrest ratified by Congress during its session of March 17, 2003.

Law no. 2004-204 dated March 9, 2004 about the adaptation of justice in regards to the evolutions of criminality. This law aims to reinforce the effectiveness of the organized rules of penal procedure applicable to delinquency and organized crime:

- The creation of specialized interregional jurisdictions;
- The installation of additional means of investigation for officers of the judiciary police (concerning the infiltration of the terrorist networks, phone-tappings, searches and police custody); and
- The extension of the statute of individuals who wish to plea bargain, which could from now on benefit from a reduction or a suspension of their sentence.
- During the judgement phase, the introduction of "appearance based on preliminary admission of guilt (guilty plea)" which offers the accused a plea bargain which includes a reduction of the sentence in exchange for an admission of facts.

"It is impossible to discuss all the rules here, such as those which authorize night searches, monitoring and surveillance and infiltration missions, the freezing of the assets of suspected indiividuals, the wiring of locals and vehicles, as well as all measures which are from this day forward under close control and scrutiny of a seated judge."[41]

In a decision dated March 2, 2004, the Constitutional Council censured 2 articles of the bill: one which prevented any possibility for future appeals from the utilization of certain methods used exclusively for the crimes committed in organized groups (gangs); the other dealt with the holding of hearings behind closed doors in the event of "guilty pleas."

French antiterrorist laws succeeded with this double challenge: in developing a French system which proved reliable while preserving fundamental freedoms even though no one can deny the recent toughening of the system.

II. The Need to Fight Efficiently Against Terrorism and the Hardening of Legislative Measures.

The important point here is to focus on the antiterrorist laws post September 11 events, and more particularly the latest to date, namely law no. 2006-64 dated January 23, 2006 relating to the fight against terrorism and which carries miscellaneous mechanisms relating to homeland security and border control, hereafter known as "law 2006." As previously noted, although we cannot talk about a circulation of the norms, we must however recognize a certain evolution, if not an unquestionable evolution, in the French antiterrorism system (A); an evolution which is nevertheless supervised (B).

A. A More Rigid Antiterrorist Judicial System.

Already, the laws from 2001 had primed a securing tendency and a report from the minstry of de-

40 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional Council,* speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.7.

41 *Ibid*, p.8.

fense titled, "Defense against terrorism: A priority of the Defense Ministry," published in April 2006,[42] confirms the above. "Since 2001, France raises the protection levels for its population and its territory." But rather, it is law 2006 which, we must admit, will demonstrate the toughening of antiterrorism laws, even if, as underlined by Nicolas Sarkozy who was then Minister of the Interior, during a speech on a proposed law.[43] Sarkozy said, "Since the attacks of September 11, several legal mechanisms - that of chapter V from the law dated Nov. 15, 2001 to the law dated March 18, 2003, for homeland security and of the law dated March 9, 2004, which adapted justice to the evolution of the criminal acts - have reinforced the state's ability to defend France against the threat of terrorism…. Toward this end, the proposed law is made-up of 15 articles contained within 8 chapters. Let us note that as recalled in the memo showing the conditions of application of law 2006[44] the latter aims to bring forth mainly the most coherent and the most complete response as possible to the threat of terrorism, both within the realm of prevention which is a more important evolution, but also in regards to certain aspects of the text regarding the repression of acts of terrorism. The law dated January 23, 2006, also had for its goal to contribute to the strengthening of the efficiency of the system of security so that it may contribute to the safeguarding of the law and order, and it contains, for this reason, certain clauses concerning the administrative police force."

This presentation of the law of 2006 is articulated around these two points: prevention and repression of the terrorist acts, the two being mixed - for once, contrary to the norm – in this last French law.

42 Ministry of Defense, http://www.defense.gouv.fr/defense/decouverte/missions/missions_generales/la_defense_contre_le_terrorism, p.7.

43 Law project related to the fight against terrorism and including various measures relative to homeland security and border control (DECLARED EMERGENCY), no. 2615, distributed on October28, 2005, p.2.

44 NOR/INT/D07/00071/C, object of circulation is the application of the number 2006-64 law signed on January 23, 2006, Paris, 21 July 2006, p.1.

Concerning Prevention

The attention of the CNIL and of miscellaneous organizations for the defense of humans rights focused, in particular, on chapter one which deals with clauses relating to video surveillance and to two main points which deserve to be underlined:

- The authorization for entities (places of worship, trades) to film the accesses to their buildings. Competent investigators will then be able to view these images (art 1).
- In case of emergency, the right granted to police commissioners (prefects) to order the installation of cameras for a period of up to 4 months, in common areas (factories, industrial or nuclear sites, train stations...).

Concerning the control of movement and travel (chapter II), the law hardens the measures adopted until then in the sense that:

- It authorizes airline, shipping and railroad companies to supply the State with personal data and other data such as the automatic monitoring of vehicles (photographs of the license plates and of the passagers in the vehicles). This database is interconnected with data files on cars flights and identity checkpoints in effect on trans-border trains.

Concerning telephone and Internet communications, (articles 5 and 6), law 2006 provides that:

- Cybercafes must save connection data (exclusive of actual contents), following the example of access suppliers. The shelf life of the saved data is requested to be one year so that competent investigators can obtain such data.

Likewise, police officers are allowed to have access, within an administrative framework, to certain files such as visa requests (BIODEV, system of delivery for visas of foreign nationals), residence permits, etc.

Concerning Repression

Law 2006, in its chapter 4 (articles 11 to 18), it supplements the penal device designated to punish acts of terrorism:

- It allows courts to repress more firmly criminal conspiracy with intent to commit acts of terrorism, when the conspiracy has for its aim to prepare for crimes or attacks upon person(s) and calls for a punishment of 20 years of incarceration, and 30 years for the leaders and organizers of such crimes.
- Likewise, the law plans for an "extradition" (centralization to the jurisdiction of the Paris district for the application of the punishment phase), for individuals condemned for acts of terrorism. This last measure, was highly criticized since it makes it nearly impossible for prisoners to stay in contact with their families, it completes the legal organization in the domain of the fight against terrorism and it centralizes the system to the French capital.
- For minors aged 16 years old or older, who are accused of acts of terrorism, they will from now on be judged by a Seated Court only made up of professional magistrates, like the Special Seated Court for the judgement of acts of terrorism commited by adults per the law of 1986. Let us note that among these magistrates must appear nevertheless, two special judges for children "the specificity of justice for minors, which constitutes one of the fundamental principles recognized by the laws of the Republic, is thus preserved."[45]
- Article 17 contains an automatic lengthening of the maximum time of custody when it has to do with terrorism, which is "increased from 4 to 6 days when the imminence of an act of terrorism is demonstrated or when the need for international co-operation requires it imperatively."[46]

In its 27th management report, the CNIL specified that "the implementation of the antiterrorist law of January 23, 2006 involved, for the past year, an increase in the number of lawful texts subjected to the CNIL and widens the possibilities of access and exploitation by police forces regarding data initially collected for another purpose. It should [also] be specified that the indication by the law itself of the conditions regarding the implementation of such law reduced the autonomy of the CNIL.[47] Alex Türk evokes "a normative wave related to the fight against terrorism," a term with which I can only agree because it is all about safety measures and not about a circulation of the standards as suggested by some lawyers, the standards (norms), according to these attorneys, being inspired by the American model. The fright inspired by the attacks of September 11, led democratic countries to reinforce their legislation as required by the need to insure public safety, a common trait to all countries. However, this reinforcement is not synonymous with a loss of our freedoms.

B.Nevertheless "Framed," and Concilliatory Efficiency and the Maintenance of a State of Human Rights.

Framed is the correct term here, because the CNIL and the constitutional Council came to agreement in regards to this law. From the very start, the CNIL worried about this above mentioned balance and the preliminary draft was subjected to serious critics: "serious risks of damage to personal freedoms," "introduction of identity checks without the knowledge of the people."

45 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional council,* speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.7.

46 NOR/INT/D07/00071/C, object of circulation is the application of law number 2006-64 voted on January 23, 2006, Paris, 21 July 2006, p.6.

47 July 9, 2007, the CNIL presented its 2006 activity report and devotes the first part "video surveillance scare" to the antiterrorist law voted on January 23, 2006, p.17.

In its opinion rendered on October 10, 2005,[48] the CNIL recalls that in accordance with the supervisory powers which were conferred to it by the law of January 6, 1978, it will not be deprived from exerting said powers fully and without restriction. This, in fact, it did not fail to do. Some of the proposals by the CNIL were taken into account during the congressional debate, including: recall of the necessity to respect data-processing laws as well as freedoms within the framework of the anti-terrorists system (except in regards to video surveillance); a clearer definition in regards to police forces and National Guard's (gendarmerie) ability to access such data with the purpose to fight terrorism; a clearer definition regarding the conditions for enabling access to such data; time limits in regards to some access; and request for an annual evaluation report to Congress.

In spite of the reservations expressed by the CNIL, other provisions of the project were not re-examined:

- systematic photographing of all vehicles and their occupants, traveling through certain major thoroughfares (this was declared to be constitutional by the Constitutional Council in its decision of January 19, 2006);
- duplication of purpose from various systems, the fight against terrorism being only one of the reasons for access to such data;
- the absence of a clear definition as to the people or entities offering access to the Internet and obligated to preserve the data in regards to connections; and
- the establishment of a central data base to control movement and travel inbound or outbound from countries located outside of the European Union, which itself has poorly defined borders.

Congressional opposition also made itself heard and in accordance with the right of "saisine" authorized by the revisions of October 29, 1974, 60 senators seized the Constitutional Council. This right of saisine of 60 representatives or senators allows a political minority to ask for the control of constitutionality of a law. The Constitutional Council, which receives an increasing number of such requests, therefore asserts itself as an effective guardian of human rights and fundamental freedoms.

Let us recall that the representatives did not hesitate to oppose this law: more than 150 amendments were recorded. The text of the law was submitted to the constitutional Council, criticizing in particular articles 6 and 8.

On January 10, 2006, the government delivered its observations regarding the opposition to this law.

Concerning article 6, which, as I am reminding you, modifies the postal service and electronic telecommunications codes, the senators, authors of "saisine," assert that the articles of this law ignore article 66 of the Constitution as well as the terms of articles 2, 4 and 16 of the Declaration of Human Rights and of the Citizen (DDHC – Declaration des Droits de l'Homme et du Citoyen - 1789, declared after the French Revolution).

Article 66 of the Constitution provides that "no one can be arbitrarily held. The legal authorities, guardian of personal freedoms, ensure the respect of this principle under the conditions as prescribed by law." To this, the government replies that the understanding of the aforesaid article leads to the following conclusion: it is the legal authorities which have an eminent role in the protection of personal freedoms. Moreover, the government specifies that it is a question of freedom in regards to not being arbitrarily detained and not the other aspects of the various individual freedoms as guaranteed by the texts and principles of constitutional value such as the freedom of coming and going, the respect of privacy, etc.

48 CNIL, http://www.cnil.fr/index.php?id=1957&delib[uid]=90&cHash=8b5071634f.

As for articles 2, 4 and 16 of the DDHC, they provide respectively that "the goal of any political group is the conservation of natural and undeniable human rights. These rights are freedom, property, security, and resistance to oppression." "Freedom consists of being able to do all that does not harm others, thus, the exercise of the natural rights of each person has limits as only within those limits which ensure that the other Members of society enjoy these same rights. These limits can be defined only by Law." "Any society in which the guarantee of such Rights is not assured, nor the separation of powers clearly defined, does not have a Constitution." It is important here, to notice, as the government in fact did, that "the damage likely to be done to privacy under the terms of article 6 of the law as submitted, remains limited." The police force and national guard do not have access to the contents of the messages being exchanged; the right to confiscate is given only to a few and clearly defined specific employees; the technical data likely to be obtained is also clearly defined and limited by law; and finally, the law specifies the methods by which such system is activated.

Concerning article 8, which puts into effect "static or mobile automated control systems with descriptive data of vehicles photographying their occupants, in all suitable points of the territory, in particular at border areas, maritime ports of entry or airports as well as on the larger axes of national or international transit." The senators brought up, once again, article 66 and article 2 of DDHC alleging that the provisions of article 8 conflicted excessively with the freedom of movement and with the respect of privacy. As recalled by the government, "on one hand...the freedom to come and go is by no means affected by the article of the law being criticized since the passive devices of automated control have neither for aim nor for effect to block the movement of people nor to limit their freedom to circulate.... In addition, it should be stressed that the damage to the rights and to the respect of privacy remains limited and that it is justified by the requirements to safeguard law and order. The point should also be made that as the systems adopted by the legislators contain many guarantees." Moreover, let us remember that "personal" data collected will be subjected to the provisions of the law of 1978 and thus to the CNIL.

On January 19, 2006, the Constitutional Council took a decision regarding the law "relating to the fight against terrorism which carried various clauses relating to security and border controls." The Constitutional Council did not declare these clauses to be unconconstitutional as they, on one hand, prove their usefullness in regards to the fight against terrorism and criminality; however, on the other hand, with the limitations and precautions with which they were issued from the point of view of the protection of privacy.

The Constitutional Council nevertheless censured the reference in regards to the "repression" of acts of terrorism as it appeared in article 6 of the law as originally submitted. The capture and processing "of traffic data," as foreseen by this article, having been born out of pure administrative police operations and having being placed solely under the responsibility of the executive power, thus do create a finality to the prevention of acts of terrorism, but they do not ignore the principle of separation of powers, nor do they encroach upon the repression of such acts, which belongs to the power of the legal authorities.

Concerning the photographing of vehicles and their occupants, the Constitutional Council estimated that, taking into account the guarantees foreseen by legislators, these measures were apt to ensure the respect of privacy and the safeguarding of law and order. Once again, you can note that the control exerted by the Constitutional Council is a control of proportionality.

As for the rest, concerning the duration of police custody in particular, neither the Constitutional Council, nor the authors of saisine, questioned it.

However, the Constitutional Council, guardian of fundamental freedoms, automatically examined these new clauses, which obviously had an impact on personal freedom. Like ourselves, Pierre Mazeaud explains,[49] "the Council evaluated them and compared them with constitutional requirements on one hand, with the need for necessary intervention by legal authorities, and the safekeeping of personal liberties under the terms of article 66 of the Constitution, on the other hand, with the need for gauging its proportionality.

The Constitutional Council validated them for the following reasons:

- these new decisions do not question any existing guarantees regarding the first four days of police custody, which the Council has already validated in its previous decisions;
- the new additional extentions can intervene only under "exceptional cases" and only in two clearly defined cases: if there "is a serious risk of imminent terrorist attack in France or abroad" or if "the needs for international co-operation requires it imperatively;"
- finally, these exceptional extentions can only be granted by justified decisions of the judge for freedoms and detention, judges which are not the same as the examining magistrate which is in charge of the control of information.

Admittedly, one can, and one must, ask oneself about the limits beyond which the duration of police custody could no longer be allowed constitutionally. If the Council considered that such limits were not crossed in fact, one could think that nevertheless we are now approaching ultimate limits, regarding said custody.

As of January 1999, the FIDH[50] (International Federation of Human Rights) had published a Report about an international investigative mission on the application of antiterrorist legislation, "*France: the door open to the arbitrary.*"[51] The latest law to date was no exception and it was spared no criticisms.

Let us recall only that the greatest infringement upon human rights is terrorism itself and that the "derogatory character of certain rules of French law in regards to the fight against terrorism must be defended,"[52] especially as this derogatory character is not synonymous with infringement of human right.

In this matter let us not suffer from a "holier than thou" syndrome; the fight against terrorism and all these miscellaneous measures, which are all geared toward optimizing the safety of the citizens, are not excessive. If the balance "safety vs. Freedom" proves to be delicate, we can only note the French system's effectiveness, combining performance and respect of the expected guarantees of a State of rights, in particular thanks to the action of the Constitutional Council and to that of the CNIL.

---

49 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional council*, speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.7.

50 The aim of the FIDH is to obtain effective improvements regarding the protection of victims, the prevention of Human Rights abuse and the prosecution of those responsible. A broad mandate – FIDH's mandate is to contribute to the respect of all rights as defined in the Universal Declaration of Human Rights. FIDH aims to obtain effective improvements in the protection of victims, the prevention of Human Rights Violations and the sanctions of their perpetrators. Its priorities are set by the triennial World Congress and the International board (22 members), with the support of the international Secretariat (30 staff members).

51 FIDH, http://www.fidh.org/IMG/pdf/france.pdf.

52 Pierre Mazeaud, *The fight against terrorism in the case law of the Constitutional council,* speech presented during a visit to the Supreme Court in Canada, April 24-26, 2006, p.3.

About the Editors

Jeffrey F. Addicott
Jeffrey F. Addicott is currently the Director of the Center for Terrorism Law at St. Mary's University School of Law (www.stmarytx.edu!ctl), San Antonio, Texas, where he teaches a variety of courses to include Terrorism Law. An active duty Army officer in the Judge Advocate General's Corps for twenty years (he retired in 2000 at the rank of Lieutenant Colonel), Professor Addicott spent a quarter of his career as a senior legal advisor to the United States Army's Special Forces.

An internationally recognized authority in terrorism law, Professor Addicott not only lectures and participates in professional and academic organizations both in the United States and abroad, he is a frequent contributor to national and international news shows to include FOX News Channel and MSNBC. Professor Addicott is a prolific author, publishing over 20 books, articles and monographs on a variety of legal topics. Among his many contributions to the field, Professor Addicott pioneered the teaching of law of war and human rights courses to the militaries of numerous nascent democracies in Eastern Europe and Latin America. For these efforts he was awarded the Legion of Merit, named the 1993 Army Judge Advocate of the year and honored as a co-recipient of the American Bar Association's Hodson award. He has served in senior legal positions in Germany, Korea, Panama and throughout the United States. Professor Addicott holds a Doctor of Juridical Science (SJD) and Master of Laws (LLM) from the University of Virginia School of Law. He also received a Master of Laws (LLM) from the Judge Advocate General's School, a Juris Doctor (JD) from the University of Alabama School of Law and a bachelor of arts with honors in government (BA) from the University of Maryland.

Ema Garcia
Ema Garcia is an associate attorney at a water law firm in Denver, Colorado. Ema holds a Juris Doctorate from St. Mary's University School of Law, a Masters of Business Administration from St. Mary's University Greehey School of Business, and a Bachelor's degree from the University of Colorado at Denver in political science. Ema also serves as a consultant for the Center for Terrorism Law where she has conducted research about bioterrorism, cyberterrorism, the freedom of information, and other various legal issues relating to terrorism.

About the Contributors

Paul D. Barkhurst
Paul has extensive litigation experience in business and real estate disputes. He has developed a special concentration in the area of eminent domain, representing governmental entities and private parties in numerous such lawsuits. Paul also represents governmental entities in construction disputes, and has represented contractors and subcontractors in private disputes. He also has extensive experience handling complex business dissolution and injunction cases. Paul began his legal career as a United States Air Force Judge Advocate General. As a JAG Captain, he prosecuted and defended numerous courts-martial trials involving felony level offenses. He finalized his military career as a Civil Litigation Attorney in Washington, D.C., representing the Air Force in federal courts throughout the country.

Richard Blum
Rick Blum is the coordinator of the Sunshine in Government Initiative, a coalition of media groups committed to promoting policies that ensure the government is accessible, accountable and open. Rick has spent the past decade in Washington advocating for the public's right to know. Prior to joining the Sunshine in Government Initiative in April 2006, Rick served as director of OpenTheGovernment.org, a broad-based national campaign to fight government secrecy. He holds a Master's Degree from Indiana University, where his studies focused on democratization efforts in Russia, and a Bachelor's degree from the University of California, Berkeley.

Jarret Brachman
Dr. Jarret Brachman is a terrorism specialist. He serves as the Director of Research in the Combating Terrorism Center at the United States Military Academy and is an Adjunct Professor at New York University's Center for Global Affairs. He has testified on terrorism related issues before the U.S. Congress, the British House of Lords and routinely advises senior military, law enforcement and intelligence officials on counterterrorism strategy. He was recently quoted by al-Qa`ida leader, Ayman al-Zawahiri.

Vanessa Brochot
Ms. Brochot is currently finishing a PhD. Her thesis focuses on "terrorism and international law." Ms. Brochot teaches French constitutional law at the University of Rouen and runs the Les Annales de Droit judicial review. Ms. Brochot has an MBA in arms control and disarmament from the University of Marne la vallée (France), a Masters degree in International Relations (D.S.R.) from the Institute of Higher Studies in International Relations in Paris (I.L.E.R.I.), and has held internships in the Ministry of Defense and the Legal Affairs Office of the French Embassy in Lima, Peru with the diplomatic chancellery as the diplomat's personal assistant.

Thomas Collins
Thomas Collins is the current Security Manager for the fourth largest water utility in the United States. His prior experiences include the creation of the first local Environmental Criminal Investi-

gation Section for the Houston Police Department in the state of Texas. Environmental Criminal Investigations turned over to the Harris County District Attorney's, Environmental Crimes Section, has resulted in the convictions of thousands of environmental criminals.

James W. Conrad, Jr.
Jamie Conrad is the principal of Conrad Law & Policy Counsel, where he provides legislative and regulatory representation to businesses, associations and coalitions in the areas of homeland security, environmental law and science policy information quality. He has spent the past 22 years practicing law in Washington, DC, most recently at the American Chemistry Council and previously at Davis, Graham & Stubbs and Cleary Gottlieb Steen & Hamilton. He is the Secretary of the ABA's Section of Administrative Law & Regulatory Practice and editor of the Environmental Science Deskbook.

Charles Davis
Charles N. Davis is executive director of the National Freedom of Information Coalition and an associate professor at the University of Missouri School of Journalism. Davis worked for nearly ten years as a journalist, working for newspapers, magazines and a news service in Georgia and Florida. As a national correspondent for Lafferty Publications, a Dublin-based news wire service for UK publications, Davis reported from the US on banking, international finance and regulatory issues for seven years before leaving full-time journalism to seek a doctorate in mass communication from the University of Florida. Davis has conducted research on dozens of freedom of information issues involving electronic access, privatization and enforcement of access laws. His 1998 study of prison access commissioned by SPJ took a year to research and earned Davis a Sunshine Award.

Maeve Dion
In early 2004, Maeve joined the CIP Program, where her work focuses on legal, economic, and policy issues relating to critical infrastructure protection. Her primary focus is on technology and information infrastructure. Maeve holds a J.D. *cum laude* from George Mason University School of Law, and an honors B.A. in political science from Eckerd College.

Stephen Gidiere
P. Stephen Gidiere III is a partner with Balch & Bingham LLP, a southeastern regional law firm with offices in Alabama, Georgia, Mississippi, and Washington, D.C. His practice encompasses a wide range of environmental, resources, energy, and administrative law matters, with a focus on government information law. He is author of the book *The Federal Information Manual* (2006) published by the American Bar Association.

Harry Hammit
Harry A. Hammitt is editor/publisher of *Access Reports*, a biweekly newsletter on the Freedom of Information Act, information policy and informational privacy issues. He is also the primary editor of *Litigation Under the Federal Open Government Laws* and the author of a series of white papers for the National Freedom of Information Coalition.

Joseph R. Larsen
Mr. Larsen is a 1990 joint JD/MBA graduate from the University of Houston Law Center and Business School, graduating in the top 10% of his law school class. Mr. Larsen, who is licensed in both Texas and Louisiana, was an editor on the University of Houston Law Review, a member of the Order of the Coif, and an associate in trial practice with Liddell, Sapp, Zivley, Hill & LaBoon, L.L.P., before joining Ogden, Gibson, White, Broocks & Longoria in 1994. His practice focus is media and access law and general and commercial litigation. He is a board member of the Freedom of Information Foundation of Texas.

Barbara Petersen
A graduate of the University of Missouri-Columbia and Florida State University College of Law, Barbara A. Petersen is president of the Florida First Amendment Foundation. Before taking her current position in 1995, Petersen was staff attorney for the Joint Committee on Information Technology Resources of the Florida Legislature, where she worked exclusively on public records legislation and issues. A passionate advocate of the public's right to oversee its government, Petersen is the author of numerous reports and articles on open government issues. She currently serves as president of the National Freedom of Information Coalition and was recently appointed chair of Florida's Commission on Open Government Reform.

Monica Schoch-Spana
Dr. Schoch-Spana, a medical anthropologist, is Senior Associate with the Center for Biosecurity of the University of Pittsburgh Medical Center (UPMC), Assistant Professor in the School of Medicine Division of Infectious Diseases, and investigator with the National Center for the Study of Terrorism and Responses to Terrorism. Since 1998, Dr. Schoch-Spana has led research, education, and advocacy efforts to encourage greater consideration by authorities of the general public's capacity to confront bioattacks and large-scale epidemics constructively. National advisory roles include serving on the Steering Committee of the Disaster Roundtable of the National Research Council (NRC) and with the NRC Committees on "Educational Paradigms for Homeland Security" and "Standards and Policies for Decontaminating Public Facilities Affected by Exposure to Harmful Biological Agents: How Clean is Safe?" Schoch-Spana received her PhD in cultural anthropology from The Johns Hopkins University.

Ari Schwartz
Ari Schwartz is the Deputy Director of the Center for Democracy and Technology (CDT). Schwartz's work focuses on increasing individual control over personal and public information. He promotes privacy protections in the digital age and expanding access to government information via the Internet. He regularly testifies before Congress and Executive Branch Agencies on these issues.

Joe Weiss
Joseph Weiss is an industry expert on control systems and electronic security of control systems, with more than 30 years of experience in the energy industry. Mr. Weiss serves as a member of numerous organizations related to control system security. These include the North American Electric Reliability Council (NERC) Critical Infrastructure Protection Committee (CIPC), the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group 15 - Data and Communication Security, the Process Controls Security Requirements Forum, CIGRÉ Joint Working Group D2/B3/C2 01- Security for Information Systems and Intranets in Electric Power Systems, and other industry working groups. He serves as the Task Force Lead for review of information security impacts on IEEE standards. He is also a Director on ISA's Standards and Practices Board.

Richard Weitz
Richard Weitz is a Senior Fellow and Director, Program Management at Hudson Institute. He analyzes mid- and long-term national and international political-military issues, including by employing scenario-based planning. His current areas of research include defense reform, counterterrorism, homeland security, and U.S. policies towards Europe, the former Soviet Union, Asia, and the Middle East. He also coordinates Hudson events and the Institute's intern program.

Pete Weitzel
Pete Weitzel is the freedom of information coordinator for the Coalition of Journalists for Open Government, based in Washington, D.C. He is a former managing editor of the Miami Herald, was the founder and first president of the Florida First Amendment Foundation and a co-founder and

president of the National Freedom of Information Coalition. He has taught at the Poynter Institute for Media Studies, University of North Carolina Journalism School and Duke University Law School.

Jody Westby

Global Cyber Risk CEO, Jody Westby, brings a seasoned, multidisciplinary perspective to the many issues facing businesses and governments today in the areas of privacy, information security, outsourcing/offshoring risks, cybercrime, and IT business risk management. Drawing upon more than twenty years of technical, legal, policy, and business experience, she regularly consults with governments, private sector executives, and operational personnel on the development of enterprise security programs that dovetail the technical, legal, operational, and managerial considerations.

Institute of Terrorism Research and Response

The staff of the Institute of Terrorism Research and Response have a broad base of military, security, and law enforcement experience, including significant experience in dealing with security issues involving municipal facilities, infrastructure venues, military installations, and public and private facilities in an environment of terrorist threats. Areas of competence at ITRR include: suicide bomber countermeasure and response, kidnapping prevention; VIP security planning; research and intelligence collection and analysis; threat and vulnerability assessments; security systems design; security management; security program plan development; crime prevention through environmental design (CPTED); knowledge of international and domestic terrorist techniques; OpSec Program Development; security assessments; integration of the human factor into the security system; anti-terrorist protective design and countermeasures; counter surveillance measures; knowledge of military demolitions techniques; special events planning; and transportation security.